Noninteractive XOR Quantum Oblivious Transfer: Optimal Protocols and Their Experimental Implementations

Lara Stroh,[1] Nikola Horová,[2] Robert Stárek,[2] Ittoop V. Puthoor,[1] Michal Mičuda,[2] Miloslav Dušek,[2] and Erika Andersson[1,*]

[1] *SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

[2] *Department of Optics, Faculty of Science, Palacký University, 17. listopadu 1192/12, Olomouc 779 00, Czech Republic*

(Received 23 September 2022; accepted 30 March 2023; published 4 May 2023)

Oblivious transfer (OT) is an important cryptographic primitive. Any multiparty computation can be realized with OT as building block. XOR oblivious transfer (XOT) is a variant where the sender Alice has two bits and a receiver Bob obtains either the first bit, the second bit, or their XOR. Bob should not learn anything more than this and Alice should not learn what Bob has learnt. Perfect quantum OT with information-theoretic security is known to be impossible. We determine the smallest possible cheating probabilities for unrestricted dishonest parties in noninteractive quantum XOT protocols using symmetric pure states and present an optimal protocol, which outperforms classical protocols. We also "reverse" this protocol, so that Bob becomes sender of a quantum state and Alice the receiver who measures it, while still implementing oblivious transfer from Alice to Bob. Cheating probabilities for both parties stay the same as for the unreversed protocol. We optically implement both the unreversed and the reversed protocols, and cheating strategies, noting that the reversed protocol is easier to implement.

DOI: 10.1103/PRXQuantum.4.020320

I. INTRODUCTION

Oblivious transfer (OT) is an important cryptographic primitive for two nontrusting parties. It is universal for multiparty computation, i.e., it can be used as a building block to implement any multiparty computation [1,2]. 1-out-of-2 oblivious transfer (1-2 OT) is probably the most well-known variant, defined by Even *et al.* [3]. Here, a sender holds two bits and a receiver obtains one of them. The sender should not know which bit the receiver has received and the receiver should only get to know one of the two bits. A few years earlier, oblivious transfer was informally described by Wiesner as a method "for transmitting two messages either but not both of which may be received" [4]. Other variants of oblivious transfer include Rabin oblivious transfer [5], 1-out-of-n oblivious transfer [6], generalized oblivious transfer [7], and XOR oblivious transfer [7].

Unfortunately, one-sided two-party computation is impossible with information-theoretic security, both in the classical and in the quantum setting [8,9]. Only with additional restrictions on dishonest parties is perfect quantum oblivious transfer possible; e.g., with bounded quantum storage [10] or relativistic constraints [11,12]. Another approach to achieve perfect quantum oblivious transfer is to assume that secure bit commitment exists [13]. Bit commitment is impossible with information-theoretic security, both in the classical and in the quantum setting, but commitment protocols with computational security are possible. The assumption of bounded quantum storage also makes bit commitment possible, essentially because adversaries can then no longer delay committing, e.g., to a choice of what measurement basis to use. Nevertheless, the cheating probabilities are bounded in quantum oblivious transfer protocols, even if the sender and receiver are only constrained by the laws of quantum mechanics. For 1-2 OT, 2/3 is a general lower bound on the greater of the sender's and the receiver's cheating probabilities [14,15]. If pure symmetric states are used to represent the sender's bit values, the bound can be increased to approximately 0.749. By combining a protocol achieving this bound with a trivial classical protocol, the cheating probabilities for both sender and receiver can be made equal to approximately 0.729 [15]. This shows that protocols using pure

*E.Andersson@hw.ac.uk

symmetric states are not optimal. However, except for 1-2 OT protocols using pure symmetric states (which are thus known to be suboptimal), there are no known quantum protocols for quantum oblivious transfer where the lower bounds have been proven to be tight.

In this paper, we focus on XOR oblivious transfer (XOT), which is less investigated but which also is universal for multiparty computation. Here, a sender holds two bits and a receiver obtains either the first bit, the second bit, or their XOR. As in 1-2 OT, the receiver should not learn anything else and the sender should not know what the receiver has learnt. To our knowledge, it is unclear whether XOT and 1-out-of-2 OT are equivalent in the quantum setting. For imperfect quantum oblivious transfer, one can argue that the "quantum advantage" is greater for noninteractive quantum XOT protocols than for noninteractive 1-out-of-2 OT protocols (see Sec. III).

We also introduce a way of "reversing" quantum oblivious transfer protocols, so that oblivious transfer can be implemented both ways, while quantum states are still sent from one party to the other party. This is of importance for applications. "Reversing" the protocol can be understood in terms of a shared entangled state, similar to how one can reimagine [16,17] the original Bennett-Brassard-84 (BB84) protocol [18] for quantum key distribution. Unlike for quantum key distribution, though, for oblivious transfer, the two parties do not trust each other. For OT, therefore, it matters who prepares the entangled state; this party could, if they so wished, prepare a different state. Cheating probabilities can therefore be different in the "original" and "reversed" protocols. For our XOT protocol, however, they turn out to be the same.

In Sec. II, we examine general noninteractive quantum XOT protocols which use pure symmetric states and give cheating probabilities for the sender and receiver. In Sec. III, we present an optimal protocol, showing that it achieves lower cheating probabilities than classical XOT protocols. Arguably, the quantum advantage is larger for XOT than for 1-2 OT. The protocol is a practical application of quantum state elimination [19,20], just as is the 1-out-of-2 OT protocol in Ref. [15], since an honest receiver needs to exclude two of the sender's four possible bit combinations. The XOT protocols are *semirandom* [15], meaning that the receiver obtains the sender's first bit, second bit, or their XOR at random. Semirandom and "standard" XOT protocols are, however, equivalent to each other with classical postprocessing; details of this are given in Appendix B.

We discuss a "reversed" version of the protocol in Sec. IV, where the sender of the quantum state becomes the receiver of a state and vice versa, while oblivious transfer is still implemented in the same direction as in the unreversed case. In the reversed protocol, the receiver similarly obtains their bit values at random. This is again equivalent to a nonrandom protocol by using classical postprocessing (see Appendix B). Finally, in Sec. V, we present the experimental implementation of both the unreversed and the reversed XOT protocols and the respective optimal cheating scenarios.

II. QUANTUM XOT WITH SYMMETRIC STATES

We consider quantum XOT protocols that satisfy certain properties.

(1) They are noninteractive protocols, where Alice sends Bob a quantum state $|\psi_{x_0x_1}\rangle$, encoding her bit values x_0, x_1, and Bob measures it.
(2) Alice's states $|\psi_{x_0x_1}\rangle$ are pure and symmetric. That is, $|\psi_{01}\rangle = U|\psi_{00}\rangle$, $|\psi_{11}\rangle = U|\psi_{01}\rangle$, and $|\psi_{10}\rangle = U|\psi_{11}\rangle$, for some unitary U with $U^4 = \hat{1}$.
(3) Each of Alice's bit combinations is chosen with probability $1/4$.
(4) When measuring each state $|\psi_{x_0x_1}\rangle$, Bob obtains x_0, x_1, or $x_2 = x_0 \oplus x_1$ with probability $1/3$.

As for the two first conditions, our results also give lower bounds on the cheating probabilities for interactive protocols, where in the last step of the protocol, Bob needs to distinguish between symmetric states. As for the two last conditions, biased protocols are of course possible but are usually not considered. Any bias can be exploited by cheating parties.

The states $|\psi_{x_0x_1}\rangle$ need to be chosen so that it is possible for Bob to obtain either x_0, x_1, or $x_2 = x_0 \oplus x_1$ correctly. We denote an honest Bob's measurement operators by Π_{0*}, Π_{1*}, Π_{*0}, Π_{*1}, $\Pi_{\mathrm{XOR}=0}$, and $\Pi_{\mathrm{XOR}=1}$, corresponding to Bob obtaining $x_0 = 0$, $x_0 = 1$, $x_1 = 0$, $x_1 = 1$, $x_2 = 0$, and $x_2 = 1$, respectively. Bob should obtain either the first or second bit, or their XOR, each with probability $1/3$. The probability of obtaining outcome m is

$$p_m = \langle\psi_{jk}|\,\Pi_m\,|\psi_{jk}\rangle\,,$$

for $m \in \{0*, 1*, *0, *1, \mathrm{XOR} = 0, \mathrm{XOR} = 1\}$. This probability should be equal to $1/3$ when an outcome is possible and otherwise be equal to 0. In Appendix A 1, we derive necessary conditions that Alice's states $|\psi_{x_0x_1}\rangle$ have to satisfy in order for Bob to be able to correctly obtain either x_0, x_1, or $x_2 = x_0 \oplus x_1$ with probability $1/3$ each. For example, it has to hold that

$$|F| \leq \frac{1}{3}, \quad |G| \leq \frac{1}{3},$$

where F and G are given by

$$\begin{aligned} &\langle\psi_{01}|\psi_{00}\rangle = \langle\psi_{11}|\psi_{01}\rangle = \langle\psi_{10}|\psi_{11}\rangle = \langle\psi_{00}|\psi_{10}\rangle = F, \\ &\langle\psi_{00}|\psi_{11}\rangle = \langle\psi_{01}|\psi_{10}\rangle = G. \end{aligned} \tag{1}$$

F is in general complex but since the states are symmetric, G must be real.

Usually, in oblivious transfer, it is assumed that the sender and receiver are choosing their inputs at random. Here, Bob will obtain either x_0, x_1, or $x_0 \oplus x_1$ at random. Using the terminology in Ref. [15], we have a semirandom XOR oblivious transfer (XOT) protocol, defined in general as follows.

Definition 1 (semirandom XOR oblivious transfer)**.** Semirandom XOT is a two-party protocol where:

(1) Alice chooses her input bits $(x_0, x_1) \in \{0, 1\}$ uniformly at random, thereby also specifying their XOR $x_2 = x_0 \oplus x_1$, or she chooses *Abort*.
(2) Bob outputs the value $b \in \{0, 1, 2\}$ and a bit y, or *Abort*.
(3) If both parties are honest, then they never abort, $y = x_b$, Alice has no information about b and Bob has no information about $x_{(b+1) \bmod 3}$ or about $x_{(b+2) \bmod 3}$.

As we show in Appendix B, implementing semirandom XOT allows us to realize standard XOT and vice versa, since these two variants of XOT are equivalent up to classical postprocessing. That is, classical postprocessing can be used to allow Bob to nevertheless make an active (but random from Alice's point of view) choice of whether he receives x_0, x_1, or $x_0 \oplus x_1$, without changing the cheating probabilities of either party.

There will be a trade-off between Alice's and Bob's cheating probabilities, as there also is for 1-2 OT [14,15,21]. Broadly speaking, when the states become more distinguishable, Bob's cheating probability increases and Alice's decreases. A cheating Bob aims to guess both x_0 and x_1, which then also implies knowledge of $x_0 \oplus x_1$; knowledge of any two bit values implies knowledge of the third one. Bob can always cheat at least with probability $1/2$ by following the protocol and randomly guessing the bit value(s) he does not obtain. It is standard to define this as "cheating." In cryptographic protocols, we are often concerned with the probability that a dishonest party will succeed in doing something they are not supposed to do. A random guess of information one does not hold, and subsequent actions using this guessed information, is a cheating strategy that is always possible. The cheating strategy that maximizes Bob's probability to correctly learn both x_0 and x_1 is evidently a minimum-error measurement. His optimal measurement is a square-root measurement [22,23], since he wants to distinguish between equiprobable, pure, and symmetric states. The square-root measurement has the measurement operators

$$\Pi_{x_0x_1} = \rho_{\text{ave}}^{-1/2} \, |\psi_{x_0x_1}\rangle \langle\psi_{x_0x_1}| \, \rho_{\text{ave}}^{-1/2},$$

where $\rho_{\text{ave}} = (1/4) \sum_{x_0x_1} |\psi_{x_0x_1}\rangle \langle\psi_{x_0x_1}|$ is the average density matrix sent to Bob by Alice. Using, e.g., an approach from Ref. [24], Bob's cheating probability can be shown to be

$$B_{\text{OT}} = \frac{1}{16} \Big| \sqrt{1 + G + 2 \operatorname{Re} F} + \sqrt{1 + G - 2 \operatorname{Re} F} + \sqrt{1 - G + 2 \operatorname{Im} F} + \sqrt{1 - G - 2 \operatorname{Im} F} \Big|^2. \quad (2)$$

When $F \to -F$, keeping G the same, Bob's cheating probability is unchanged. For fixed $|F|$ and $|G|$, Bob's cheating probability is minimized for real F if $G \leq 0$ and for purely imaginary F if $G \geq 0$. One way to see this is to examine $\sqrt{B_{\text{OT}}}$ as a function of θ_F, with $F = |F| e^{i\theta_F}$; it is easy to verify that the maxima and minima of this function are as just described. Broadly speaking, Bob's cheating probability increases with decreasing $|F|$ and $|G|$, which means that the states become more distinguishable. If $F = G = 0$, the states are perfectly distinguishable and Bob's cheating probability is equal to 1. If $|F| = |G| = 1$, Bob's cheating probability as given by Eq. (2) would be equal to $1/4$. Bob's cheating probability will, however, never be this low, since the states $|\psi_{x_0x_1}\rangle$ have to be chosen so that Bob can obtain one of Alice's bits correctly. As mentioned above, even with a random guess, Bob can also always cheat at least with probability $1/2$. Since it has to hold that $|F|, |G| \leq 1/3$ (see Appendix A 1), Bob's cheating probability is in fact never lower than $3/4$. This occurs for $F = \pm 1/3$, $G = -1/3$ and for $F = \pm i/3$, $G = 1/3$.

A cheating Alice aims to guess whether Bob has obtained x_0, x_1, or $x_2 = x_0 \oplus x_1$. Even if following the protocol, Alice can always cheat at least with probability $1/3$ with a random guess. One can consider two different types of protocol. Either Bob does not test the states Alice sends to him, in which case a dishonest Alice can send him any state; or, similar to the procedure in the 1-2 OT protocol in Ref. [15], Alice can send Bob a sequence of states and Bob asks her to declare what a fraction of them are. Bob then checks that his measurement results agree with Alice's declaration, which can restrict Alice's available cheating strategies. In the latter scenario, it is Alice's average cheating probability that is bounded, instead of her cheating probability for each individual position. Generally, Alice's cheating probability when Bob does not test is at least as high as when he does test.

In the case when Bob tests a fraction of the states that she sends him, a dishonest Alice must use an equal superposition of the states that she is supposed to send, entangled with a system that she keeps on her side, in order to pass Bob's tests. In Appendix A 2, we show that when Bob is testing Alice's states, her cheating probability is bounded as

$$A_{\text{OT}} \geq \begin{cases} \frac{1}{3} + \frac{1}{2}|\operatorname{Im} F| + \frac{1}{2} \max(|\operatorname{Re} F|, |G|), & \text{if } G \leq 0, \\ \frac{1}{3} + \frac{1}{2}|\operatorname{Re} F| + \frac{1}{2} \max(|\operatorname{Im} F|, |G|), & \text{if } G > 0. \end{cases} \quad (3)$$

As expected, the bound on Alice's cheating probability increases with larger $|F|$ and $|G|$. The bound is also

unchanged if $F \to -F$, keeping G the same. Now suppose that we fix $|F|$ and $|G|$. If $G < 0$, we see that we should choose Im $F = 0$ in order to minimize the bound on Alice's cheating probability and if $G > 0$, we should choose Re $F = 0$. If $G = 0$, a real F and a purely imaginary F with the same $|F|$ will give the same bound. As we have already seen, if $|F|$ and $|G|$ are fixed, also Bob's cheating probability is minimized for these same choices of θ_F. The analysis of Alice's cheating probability when Bob is not testing her states below will further confirm that these are the optimal choices of θ_F for quantum XOT protocols using symmetric pure states.

While the bound on Alice's cheating probability in Eq. (3) increases with $|F|$ and $|G|$, Bob's cheating probability in Eq. (2) is larger for smaller $|F|$ and $|G|$. Together, Eqs. (2) and (3) give a trade-off relation between Alice's and Bob's cheating probabilities for noninteractive quantum XOT protocols using pure symmetric states when Bob is testing Alice's states.

When Bob is not testing, it is optimal for Alice to send him the pure state, within the subspace spanned by the states that she is supposed to send him, for which Bob's probability of obtaining either x_0, x_1, or x_2 is maximized. In Appendix A 3, we show that the largest $p(x_0)$ and $p(x_1)$ Alice can achieve is equal to

$$p(x_0)_{\max} = p(x_1)_{\max} = \max(\tilde{\lambda}_{00}, \tilde{\lambda}_{01}), \tag{4}$$

where

$$\tilde{\lambda}_{00} = \frac{1}{(1+G)^2 - 4(\mathrm{Re}\,F)^2}\left[\frac{1}{3}(1+G) - 2(\mathrm{Re}\,F)^2 + \sqrt{\left(\frac{1}{3}+G\right)^2(\mathrm{Re}\,F)^2 + [(1+G)^2 - 4(\mathrm{Re}\,F)^2](\mathrm{Im}\,F)^2}\right],$$
$$\tilde{\lambda}_{01} = \frac{1}{(1-G)^2 - 4(\mathrm{Im}\,F)^2}\left[\frac{1}{3}(1-G) - 2(\mathrm{Im}\,F)^2 + \sqrt{\left(\frac{1}{3}-G\right)^2(\mathrm{Im}\,F)^2 + [(1-G)^2 - 4(\mathrm{Im}\,F)^2](\mathrm{Re}\,F)^2}\right], \tag{5}$$

and the largest $p(x_2)$ is

$$p(x_2)_{\max} = \begin{cases} \frac{1/3+G}{1+G-2|\mathrm{Re}\,F|}, & \text{if } G \geq \frac{|\mathrm{Im}\,F|-|\mathrm{Re}\,F|}{2-3|\mathrm{Re}\,F|-3|\mathrm{Im}\,F|}, \\ \frac{1/3-G}{1-G-2|\mathrm{Im}\,F|}, & \text{if } G < \frac{|\mathrm{Im}\,F|-|\mathrm{Re}\,F|}{2-3|\mathrm{Re}\,F|-3|\mathrm{Im}\,F|}. \end{cases} \tag{6}$$

Alice's overall cheating probability is then the larger of $p(x_0)_{\max} = p(x_1)_{\max}$ and $p(x_2)_{\max}$.

The expressions for $p(x_0)$ and $p(x_1)$ in Eq. (5) are somewhat complicated but can be numerically investigated and plotted. In Fig. 1, we plot Alice's cheating probabilities for $G = -1/3$, $G = -1/6$, and $G = 0$. One can note that $p(x_i)_{\max}$ do not depend on the sign of Re F and Im F and that Alice's cheating probabilities are unchanged if Re F and Im F are interchanged, with G changing to $-G$.

When F is real, Alice's cheating probabilities reduce to

$$p(b=0)_{\max} =$$
$$p(b=1)_{\max} = \begin{cases} \text{(i) } \frac{1/3+|F|}{1-G}, & \text{if } G \geq -|F|, \\ \text{(ii) } \frac{1/3+|F|}{1+G+2|F|}, & \text{if } G \leq -|F| \end{cases} \tag{7}$$

and

$$p(b=2)_{\max} = \begin{cases} \text{(iii) } \frac{1/3+G}{1+G-2|F|}, & \text{if } G \geq \frac{-|F|}{2-3|F|}, \\ \text{(iv) } \frac{1/3-G}{1-G}, & \text{if } G \leq \frac{-|F|}{2-3|F|}. \end{cases} \tag{8}$$

Alice's overall cheating probability is again the largest of the four expressions in Eqs. (7) and (8). For $G \leq -|F|$, the largest probability is expression (iv) for $p(b=2)$, and for $G \geq -|F|$, the largest expression is either expression (i) for $p(b=0)_{\max} = p(b=1)_{\max}$ or expression (iii) for $p(b=2)$, depending on F and G. Expression (i) is greater than (iii) when $G > |F|$ or $G < 1/3 - 2|F|$. This means that in the region $F > 0$, (iii) is the largest expression in the hourglass-shaped region in between the lines $G = F$ and $G = 1/3 - 2F$ and (i) is the largest expression in the two wedges at either side (see Fig. 2). In the region $F < 0$, the hourglass and wedges are instead formed by the lines $G = -F$ and $G = 1/3 + 2F$.

Broadly speaking, Alice's cheating probability increases when $|F|$ and $|G|$ increase, that is, when the states that she sends become less distinguishable to Bob; this is also the case for a cheating Alice when Bob does test. Bob's cheating probability in Eq. (2) is never smaller than 3/4. This occurs for $F = \pm 1/3$, $G = -1/3$ and for $F = \pm i/3$, $G = 1/3$. In all of these cases, Alice's cheating probability is equal to 1/2, irrespective of whether Bob tests her states or not. Her cheating probability can be made smaller than 1/2, at the expense of further increasing Bob's cheating probability, which already is relatively large at 3/4. In Ref. [25], Osborn and Sikora present general lower bounds for Alice's and Bob's cheating probabilities in quantum XOT, that is, $B_{\mathrm{OT}} \gtrapprox 0.5073$ or $A_{\mathrm{OT}} \gtrapprox 0.3382$. It

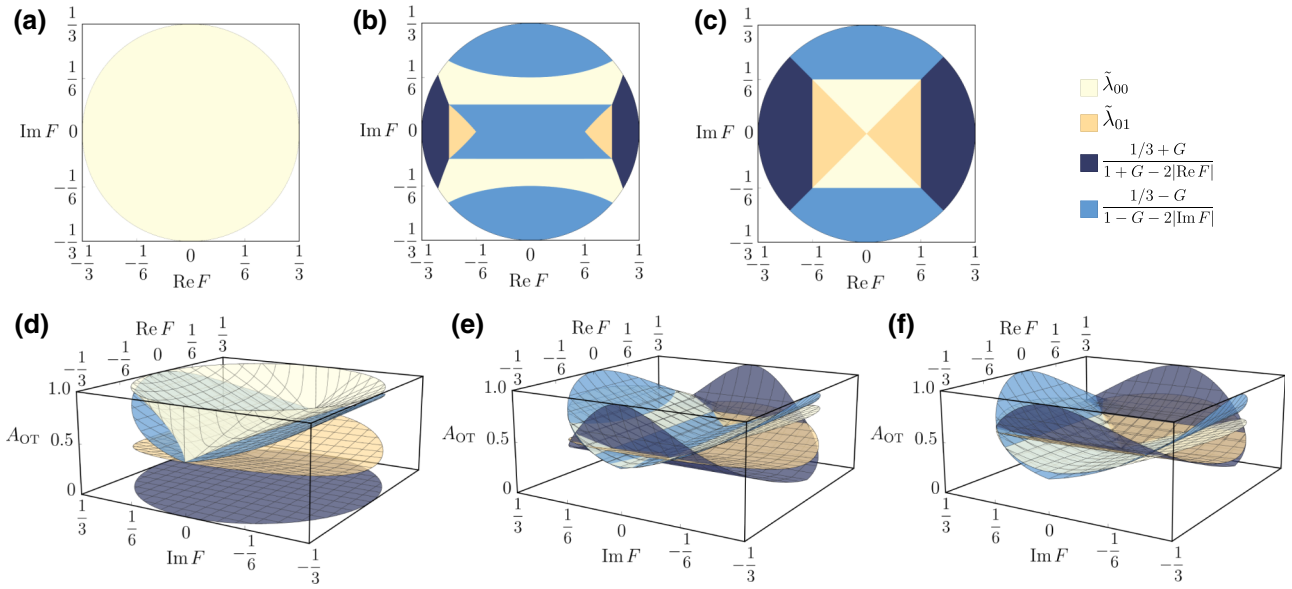

FIG. 1. Alice's optimal cheating probabilities in Eqs. (5) and (6) for different values of G: (a),(d) $G = -1/3$; (b),(e) $G = -1/6$; (c),(f) $G = 0$. The plots (a)–(c) show top-down views of (d)–(f), respectively.

is, however, not known if protocols exist that are tight with those bounds. The expressions in Eq. (2) and Eqs. (3)–(6) give actual cheating probabilities, not bounds, as a function of the pairwise overlaps between the states that an honest Alice sends.

III. A NONINTERACTIVE QUTRIT XOT PROTOCOL

We present a protocol that can thus be said to be optimal among noninteractive protocols using pure symmetric states, since it achieves the smallest possible cheating probability 3/4 for Bob and the smallest possible cheating probability 1/2 for Alice, given that Bob's cheating probability is 3/4. In our protocol, Alice encodes two bit values x_0 and x_1 in one of the four nonorthogonal states

$$|\phi_{x_0x_1}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + (-1)^{x_1}|1\rangle + (-1)^{x_0}|2\rangle). \quad (9)$$

These states are symmetric, in the sense that $|\phi_{01}\rangle = U|\phi_{00}\rangle$, $|\phi_{11}\rangle = U^2|\phi_{00}\rangle$, and $|\phi_{10}\rangle = U^3|\phi_{00}\rangle$ for

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad (10)$$

for which it holds that $U^4 = \hat{1}$. The states $|\phi_{x_0x_1}\rangle$ are selected so that it is possible to unambiguously exclude two of them, meaning that it is possible to learn either x_0, x_1, or $x_0 \oplus x_1$. Because the states are nonorthogonal, it is not possible to unambiguously determine which single

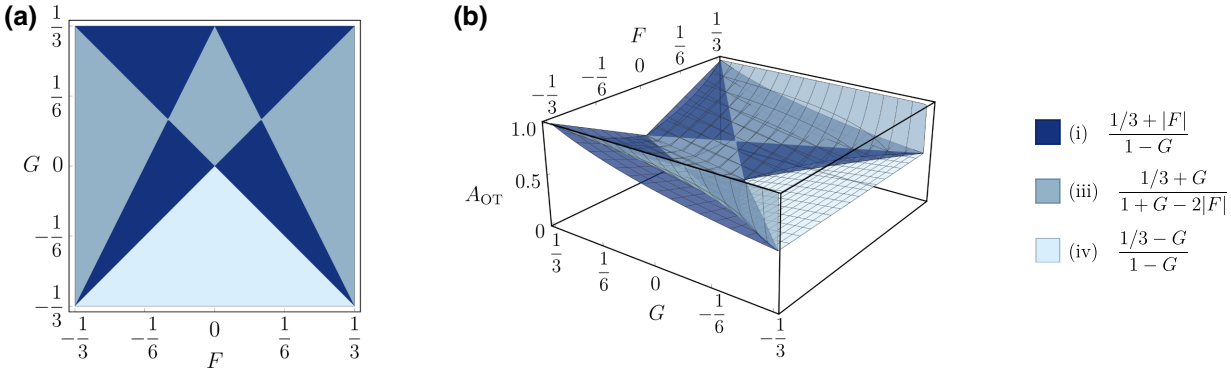

FIG. 2. Alice's optimal cheating probabilities for real F in Eqs. (7) and (8). The region plot in (a) is the top view of the 3D plot in (b), both showing the regions for which (i), (iii), or (iv) are the largest, respectively.

TABLE I. Bob's measurement operators and outcomes.

Outcome bit	Eliminated states	Measurement operator
$x_0 = 0$	$\|\phi_{11}\rangle$ and $\|\phi_{10}\rangle$	$\Pi_A = \frac{1}{4}(\|0\rangle + \|2\rangle)(\langle 0\| + \langle 2\|)$
$x_0 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{01}\rangle$	$\Pi_B = \frac{1}{4}(\|0\rangle - \|2\rangle)(\langle 0\| - \langle 2\|)$
$x_1 = 0$	$\|\phi_{11}\rangle$ and $\|\phi_{01}\rangle$	$\Pi_C = \frac{1}{4}(\|0\rangle + \|1\rangle)(\langle 0\| + \langle 1\|)$
$x_1 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{10}\rangle$	$\Pi_D = \frac{1}{4}(\|0\rangle - \|1\rangle)(\langle 0\| - \langle 1\|)$
$x_2 = 0$	$\|\phi_{01}\rangle$ and $\|\phi_{10}\rangle$	$\Pi_E = \frac{1}{4}(\|1\rangle + \|2\rangle)(\langle 1\| + \langle 2\|)$
$x_2 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{11}\rangle$	$\Pi_F = \frac{1}{4}(\|1\rangle - \|2\rangle)(\langle 1\| - \langle 2\|)$

state was received, meaning that it is impossible for Bob to perfectly learn both bits x_0 and x_1.

After choosing her bits $(x_0, x_1) \in \{0, 1\}$ uniformly at random, Alice sends the respective state to Bob, who makes an unambiguous quantum state elimination measurement to exclude two of the four possible states. There are six different pairs of states that he can exclude. Each excluded pair corresponds to learning either x_0, x_1, or $x_0 \oplus x_1$, with either the value 0 or 1. To construct Bob's measurement operators, we need six states, each one orthogonal to a pair of states in Eq. (9). The measurement operators are then proportional to projectors onto these six states, normalized so that their sum is equal to the identity matrix. For instance, the measurement operator $\Pi_A = (1/4)(|0\rangle + |2\rangle)(\langle 0| + \langle 2|)$ will exclude the states $|\phi_{11}\rangle$ and $|\phi_{10}\rangle$, so that Bob's outcome bit will be $x_0 = 0$, and similarly for the other operators. Table I gives the excluded pairs, the corresponding measurement operators, and the deduced output bits for Bob.

To summarize, our XOT protocol proceeds as follows:

(1) The sender Alice uniformly at random chooses the bits $(x_0, x_1) \in \{0, 1\}$ and sends the corresponding state $|\phi_{x_0 x_1}\rangle$ to the receiver Bob.
(2) Bob performs an unambiguous state elimination measurement, excluding two of the possible states with certainty, from which he can deduce either x_0, x_1, or $x_2 = x_0 \oplus x_1$.

Bob's and Alice's cheating probabilities are obtained from the expressions in Eq. (2) and Eqs. (3)–(6), with $F = 1/3$ and $G = -1/3$. A dishonest Bob can cheat with probability $B_{\mathrm{OT}} = 3/4$. Alice's cheating probability is $A_{\mathrm{OT}} = 1/2$, whether or not Bob tests the states that Alice sends. Our noninteractive XOT protocol has the same cheating probabilities as protocol (3) given by Kundu *et al.* [26]. That protocol, however, uses entanglement and is interactive, that is, quantum states are sent back and forth between sender and receiver. Our protocol achieves the same cheating probabilities but is easier to implement, since it is noninteractive and does not require entanglement. In Appendix C, we show how our protocol can be related to the protocol in Ref. [26].

A. Comparison to classical XOT protocols

To compare our quantum XOT protocol to classical protocols, we consider a combination of two trivial classical XOT protocols. In one, Alice can cheat perfectly and in the other, Bob can cheat perfectly, similarly to the two "bad" classical XOT protocols presented in Ref. [26].

Protocol 1. Alice has the two bits (x_0, x_1) and chooses to send Bob either x_0, x_1, or $x_2 = x_0 \oplus x_1$. Subsequently, Alice "forgets" what she has done.

Obviously, in this protocol, Alice can cheat with probability 1, while Bob can only cheat with probability 1/2. This is his probability to correctly guess the value of the bit that he did not receive and the XOR of Alice's bits.

Protocol 2. Alice sends all of $(x_0, x_1, x_2 = x_0 \oplus x_1)$ to Bob, who chooses to read one of these bits and discards the other two without looking at them.

Obviously, Bob can now cheat with probability 1, since he could read out both x_0 and x_1. Alice, on the other hand, can only cheat with probability 1/3 by guessing which bit Bob has chosen to read out.

Protocol 3 is a combination of Protocols 1 and 2, following Ref. [14]. Alice and Bob conduct an unbalanced weak coin-flipping protocol. Its outcome will specify which of the two protocols is implemented. The result is effectively as follows.

Protocol 3. Protocol 1 is implemented with probability s and Protocol 2 is implemented with probability $(1 - s)$.

The cheating probabilities for Alice and Bob in Protocol 3 are given by

$$A^c_{\mathrm{OT}} = \frac{1}{3} + \frac{2}{3}s \quad \text{and} \quad B^c_{\mathrm{OT}} = 1 - \frac{1}{2}s. \tag{11}$$

Eliminating s, we obtain the trade-off relation

$$3A^c_{\mathrm{OT}} + 4B^c_{\mathrm{OT}} = 3\left(\frac{1}{3} + \frac{2}{3}s\right) + 4\left(1 - \frac{1}{2}s\right) = 5. \tag{12}$$

If a quantum protocol achieves $3A_{\mathrm{OT}} + 4B_{\mathrm{OT}} < 5$, it has a quantum advantage. As shown earlier, we have $A_{\mathrm{OT}} = 1/2$ and $B_{\mathrm{OT}} = 3/4$ in our quantum XOT protocol. Thus, we obtain $3A_{\mathrm{OT}} + 4B_{\mathrm{OT}} = 9/2 < 5$, meaning that it beats the considered classical protocols.

Arguably, the quantum advantage is larger for XOT than for 1-out-of-2 OT, where analogously defined classical protocols satisfy $A_{\mathrm{OT}} + B_{\mathrm{OT}} = 3/2$ and a quantum protocol achieves $A_{\mathrm{OT}} + B_{\mathrm{OT}} \approx 3/4 + 0.729 = 1.479$ [15]. Since 1-out-of-2 OT and XOT are different functionalities, we cannot directly compare their trade-off relations

and quantum advantages in cheating probabilities. However, we can make a reasonable comparison as follows. The lhs in the trade-off relation in Eq. (12) for XOT is $3A^c_{\mathrm{OT}} + 4B^c_{\mathrm{OT}}$, which would take the maximal value of 7 if both Alice and Bob could cheat perfectly: $A_{\mathrm{OT}} = B_{\mathrm{OT}} = 1$. The corresponding maximal value in the trade-off relation $A_{\mathrm{OT}} + B_{\mathrm{OT}} = 3/2$ for "classical" 1-out-of-2 OT is 2. It would therefore not be fair to directly compare the difference between 5 and 9/2 (between the rhs in Eq. (12) and the value 9/2 achieved for our quantum XOT protocol) with the difference between 3/2 and 1.479 (which are the corresponding values for classical and quantum 1-out-of-2 OT). But if we multiply the difference for the XOT protocol by 2 and the difference for the 1-out-of-2 protocol by 7, the comparison can be said to be fair. That is, since $(5 - 9/2) \times 2 = 1 > (3/2 - 1.479) \times 7 = 0.147$, it is justifiable to say that the quantum advantage is larger for XOT than for 1-out-of-2 OT. We could also make the comparison instead using the cheating probabilities in ideal protocols. For ideal XOT, we have $A_{\mathrm{OT}} = 1/3$ and $B_{\mathrm{OT}} = 1/2$, giving $3A_{\mathrm{OT}} + 4B_{\mathrm{OT}} = 3$ as the rhs of the trade-off relation. For an ideal 1-out-of-2 OT protocol, we have $A_{\mathrm{OT}} = B_{\mathrm{OT}} = 1/2$ and $A_{\mathrm{OT}} + B_{\mathrm{OT}} = 1$. The "scaled" quantum advantages then become $5 - 9/2 = 1/2$ for XOT, which is greater than $(3/2 - 1.479) \times 3 = 0.063$ for 1-out-of-2 OT.

We also note that the bounds on cheating probabilities for XOT hold for every individual implementation of the protocol, while for the 1-out-of-2 OT protocol in Ref. [15], the bound is only for the average cheating probability. In particular, the sender could cheat perfectly in any individual 1-out-of-2 OT round, with a negligible probability of being caught, as long as they cheat only in a sufficiently small number of rounds. In this sense too, XOT gives a greater quantum advantage than the 1-out-of-2 quantum OT protocol in Ref. [15].

IV. "REVERSING" THE XOT PROTOCOL

It is useful to be able to implement oblivious transfer between two parties "both ways." One party might only be able to prepare and send quantum states and the other party might only be able to detect them. This has also been noted in Ref. [27]. We now show that it is possible to "reverse" our noninteractive protocol, so that XOR oblivious transfer from Bob to Alice can be achieved by Alice sending quantum states to Bob, who measures them. Alternatively, XOR oblivious transfer from Alice to Bob can be implemented by Bob sending quantum states to Alice, who measures them. Such a "reversal" of a noninteractive quantum OT protocol, using the procedure we describe, is generally possible, but cheating probabilities may be different in the "original" and "reversed" protocols. For our specific XOT protocol, we show that they nevertheless end up being the same.

We consider noninteractive XOT from Alice to Bob, implemented so that Bob sends Alice one of six states depending on his randomly chosen x_0, x_1, or $x_2 = x_0 \oplus x_1$ and its value. Alice learns x_0 and x_1 by performing a measurement on Bob's state. For the reversed noninteractive XOT protocol, Bob's measurement operators given in Table I become his states, when normalized to 1, and Alice's states given in Eq. (9) become her measurement operators, when renormalized so that they sum to the identity operator. The XOT protocol is then performed as follows:

(1) Bob randomly chooses one of the six states

$$\begin{aligned}
|\phi_{x_0=0}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle),\\
|\phi_{x_0=1}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle),\\
|\phi_{x_1=0}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\\
|\phi_{x_1=1}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\\
|\phi_{x_2=0}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle),\\
|\phi_{x_2=1}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)
\end{aligned} \tag{13}$$

and sends it to Alice. This choice determines the values of b and bit x_b, i.e., Bob's input and output in "standard" nonrandom XOT.

(2) Alice performs a measurement on the state that she has received from Bob, learning the bit values (x_0, x_1). Her measurement operators $\Pi_{x_0x_1}$ are

$$\begin{aligned}
\Pi_{00} &= \frac{1}{4}(|0\rangle + |1\rangle + |2\rangle)(\langle 0| + \langle 1| + \langle 2|),\\
\Pi_{01} &= \frac{1}{4}(|0\rangle - |1\rangle + |2\rangle)(\langle 0| - \langle 1| + \langle 2|),\\
\Pi_{11} &= \frac{1}{4}(|0\rangle - |1\rangle - |2\rangle)(\langle 0| - \langle 1| - \langle 2|),\\
\Pi_{10} &= \frac{1}{4}(|0\rangle + |1\rangle - |2\rangle)(\langle 0| + \langle 1| - \langle 2|).
\end{aligned} \tag{14}$$

In terms of x_0 and x_1, Alice's measurement operators can be written $\Pi_{x_0x_1} = |\Phi_{x_0x_1}\rangle\langle\Phi_{x_0x_1}|$, where $|\Phi_{x_0x_1}\rangle = (1/2)(|0\rangle + (-1)^{x_1}|1\rangle + (-1)^{x_0}|2\rangle)$. As in the unreversed XOT protocol, when both parties act honestly, Alice will have two bits, but will not know whether Bob knows her first bit, her second bit, or their XOR. Bob will have one of x_0, x_1, or $x_2 = x_0 \oplus x_1$ but will not know anything else, since he can only deduce one bit of information with certainty, based on the state that he has sent (if he is honest).

In the reversed XOT protocol, Alice cannot choose her bit values, whereas in the unreversed protocol, Bob could not directly choose b. However, as for the unreversed protocol, it is possible to add classical postprocessing to turn the reversed protocol into "standard" nonrandom XOT, where Alice can choose her bit values and where Bob can consequently only choose b but not the value of the bit that he obtains. In Appendix B, we describe this classical postprocessing as well.

The aim of cheating parties in the reversed protocol stays unchanged, i.e., dishonest Alice still wants to learn which output Bob has obtained and dishonest Bob still wants to learn not just one bit but any two of x_0, x_1, or $x_0 \oplus x_1$. In the reversed protocol, he wants to know exactly which of the four two-bit combinations Alice has obtained. The cheating probabilities are derived in Appendix D. Alice cheats by distinguishing between the three mixed states obtained by pairing up the states in Eq. (13) that correspond to the same output. A minimum-error measurement gives her a cheating probability of $A^r_{\mathrm{OT}} = 1/2$. As in the unreversed protocol, for the cheating sender of the state (now Bob), there are two scenarios: one where the receiver of the state (now Alice) tests the state and another where she does not test. Also here, Bob's cheating probability for both scenarios is the same, that is, we have $B^r_{\mathrm{OT}} = 3/4$ in both cases. When Alice is not testing, Bob can achieve this by sending an eigenvector corresponding to the largest eigenvalue of one of Alice's measurement operators. If Alice does test, however, he needs to send a superposition of the states he is supposed to send, entangled with some system that he keeps.

All in all, we have a noninteractive reversed XOT protocol, implementing XOT from a party who only needs to detect quantum states to a party who only needs to send states. The receiver of the quantum states does not need to test a fraction of the received states. The cheating probabilities for the two parties are the same as in the unreversed version of the protocol.

A. Original and reversed protocols in terms of a shared entangled state

Instead of preparing and sending one of the states $|\phi_{x_0x_1}\rangle$ as in the original protocol, Alice could prepare the state

$$|\Psi_{\mathrm{ent}}\rangle_{AB} = \frac{1}{2}\left(|a\rangle_A |\phi_{00}\rangle_B + |b\rangle_A |\phi_{01}\rangle_B + |c\rangle_A |\phi_{11}\rangle_B + |d\rangle_A |\phi_{10}\rangle_B\right), \tag{15}$$

where $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ is an orthonormal basis for a system that she keeps on her side. She sends the B system to Bob. If Alice measures the A system in the $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ basis, then this prepares one of the states $|\phi_{x_0x_1}\rangle_B$ on Bob's side. From both Bob's and Alice's viewpoints, this is equivalent to the original protocol and their cheating probabilities remain the same. Using the definitions of $|\phi_{x_0x_1}\rangle$ in Eq. (9), the entangled state in Eq. (15) can also be written

$$|\Psi_{\mathrm{ent}}\rangle_{AB} = \frac{1}{\sqrt{3}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B + |2\rangle_A |2\rangle_B),$$

where

$$\begin{aligned}
|0\rangle_A &= \frac{1}{2}(|a\rangle_A + |b\rangle_A + |c\rangle_A + |d\rangle_A),\\
|1\rangle_A &= \frac{1}{2}(|a\rangle_A - |b\rangle_A - |c\rangle_A + |d\rangle_A),\\
|2\rangle_A &= \frac{1}{2}(|a\rangle_A + |b\rangle_A - |c\rangle_A - |d\rangle_A),\\
|3\rangle_A &= \frac{1}{2}(|a\rangle_A - |b\rangle_A + |c\rangle_A - |d\rangle_A),
\end{aligned} \tag{16}$$

are orthonormal states and we define a fourth basis ket $|3\rangle_A$. Both Alice's and Bob's state spaces for the state $|\Psi_{\mathrm{ent}}\rangle_{AB}$ are three dimensional; its Schmidt number is 3. Alice's measurement in the $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ basis can be understood as a realization, with a Neumark extension using the auxiliary basis state $|3\rangle_A$, of her generalized quantum measurement in the "reversed" protocol, with measurement operators given in Eq. (14).

If, instead, Bob prepares the state $|\Psi_{\mathrm{ent}}\rangle_{AB}$, sends the A system to Alice, and measures his B system using the measurement that he makes in the original protocol, then this prepares one of the states $|\phi_{x_i=b}\rangle$ on Alice's side. This is equivalent to the reversed protocol. That is, starting from the entangled state $|\Psi_{\mathrm{ent}}\rangle_{AB}$, either the original or the reversed protocol can be implemented. In both cases, Alice makes the measurement she would make in the reversed protocol and Bob makes the measurement he would make in the original protocol. What determines whether the procedure is equivalent to the original or reversed protocol is who prepares the state $|\Psi_{\mathrm{ent}}\rangle_{AB}$. This matters, because Alice and Bob are not guaranteed to follow the protocol and could prepare some other state if they were dishonest.

In order to illustrate the generality of this procedure, let us "reverse" the protocol in Ref. [15]. Here, Alice sends one of the two-qubit states $|0\rangle|0\rangle$, $|+\rangle|+\rangle$, $|1\rangle|1\rangle$, or $|-\rangle|-\rangle$ to Bob, encoding her bit values 00, 01, 11, and 10, respectively, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Since each of Alice's four states are symmetric under exchange of the two qubits, the state space is actually three dimensional. Bob measures one qubit in the $|0\rangle, |1\rangle$ basis and the other one in the $|+\rangle, |-\rangle$ basis, which allows him to rule out two of the four possible states, so that he can infer the value of either Alice's first bit or her second bit (never their XOR). Here, we use an equivalent set of four states with the same

pairwise overlaps,

$$|\phi'_{x_0x_1}\rangle = \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_1}\frac{1}{2}|1\rangle + (-1)^{x_0}\frac{1}{2}|2\rangle, \quad (17)$$

making it immediately clear that the state space is three dimensional. Alice could now instead prepare the state

$$\begin{aligned}|\Phi'_{\text{ent}}\rangle &= \frac{1}{2}(|a\rangle_A|\phi'_{00}\rangle_B + |b\rangle_A|\phi'_{01}\rangle_B \\ &\quad + |c\rangle_A|\phi'_{11}\rangle_B + |d\rangle_A|\phi'_{10}\rangle_B) \\ &= \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{2}|1\rangle_A|1\rangle_B + \frac{1}{2}|2\rangle_A|2\rangle_B, \quad (18)\end{aligned}$$

with the same definition of the states $|0\rangle_A$, $|1\rangle_A$, and $|2\rangle_A$ as in Eq. (16), and send the B system to Bob. If Alice measures the A system in the $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ basis—or makes the equivalent four-outcome generalized measurement in the three-dimensional (3D) space spanned by the states $|0\rangle_A$, $|1\rangle_A$, and $|2\rangle_A$—then this prepares one of the states $|\phi'_{x_0x_1}\rangle$ on Bob's side. This is then equivalent to Alice's actions in the protocol in Ref. [15]. Preparing the above entangled state is also how a dishonest Alice would cheat in Ref. [15]. She can then always revert to effectively sending Bob one of the states that she should have sent him, if Bob decides to test the state that she has sent. If she does go ahead with cheating, she measures the A system in a way that optimally lets her deduce which bit value (x_0 or x_1) Bob has obtained, in which case she can learn this with probability 3/4. If Bob does not test the states that Alice sends, one can show that she can in fact cheat with probability 1 (and that it does not help if Bob randomly chooses which qubit he measures in what basis). If Bob is dishonest, he can determine which one of the four states $|\phi'_{x_0x_1}\rangle$ Alice has sent him with probability approximately 0.729.

If, instead, Bob were to prepare the entangled state and send the A system to Alice, we would obtain a reversed version of the protocol in Ref. [15]. One can show that the measurement that an honest Bob makes prepares one of the four states

$$\begin{aligned}|\phi'_{x_0=0}\rangle &= \frac{1}{\sqrt{2}}(|a\rangle_A + |b\rangle_A), \\ |\phi'_{x_1=0}\rangle &= \frac{1}{\sqrt{2}}(|a\rangle_A + |d\rangle_A), \\ |\phi'_{x_0=1}\rangle &= \frac{1}{\sqrt{2}}(|c\rangle_A + |d\rangle_A), \\ |\phi'_{x_1=1}\rangle &= \frac{1}{\sqrt{2}}(|b\rangle_A + |c\rangle_A)\end{aligned} \quad (19)$$

on Alice's side. If Bob is dishonest, he can send Alice some other state(s) in the three-dimensional state space spanned by these states; the state $(|a\rangle_A - |b\rangle_A - |c\rangle_A + |d\rangle_A)/2$ is orthonormal to all of the above four states. It is necessary to reanalyze what the cheating probabilities are in the reversed 1-2-OT protocol, since they may change when a protocol is reversed. Bob's cheating probability could increase, since more cheating strategies are available to him, while Alice's cheating probability could decrease. In this case, it can be shown that Alice's cheating probability is 3/4, the same as in the unreversed protocol when Bob was testing the states that she sends. Bob's cheating probability increases to 3/4 if Alice does not test the states that he sends and is equal to 0.729 if Alice does test the states that he sends (the same as Bob's cheating probability in the unreversed protocol).

V. EXPERIMENT

A. Both parties honest

In the case where both parties are honest, Alice prepares one of the qutrit states given in Eq. (9) and sends it to Bob. In our experimental implementation, these states are encoded into spatial and polarization degrees of freedom of a single photon using the setup depicted in Alice's part of Fig. 3, which consists of half-wave plates and a calcite beam displacer (it shifts the horizontally polarized beam). The basis state $|0\rangle$ is represented by the horizontally polarized mode in the upper output, $|1\rangle$ by the horizontally polarized mode in the lower output, and $|2\rangle$ by the vertically polarized mode in the lower output. The photons incoming from a single-photon source have a horizontal linear polarization. The settings of the angles of the waveplate axes corresponding to all of Alice's states are listed in Table II.

Bob's six measurement operators are defined in Table I, for unambiguously eliminating pairs of states. This measurement can be implemented by a projective von Neumann measurement $\{|\xi_i\rangle\langle\xi_i|\}_{i=A}^{F}$ in an extended six-dimensional Hilbert space, where

$$\begin{aligned}|\xi_A\rangle &= \frac{1}{2}(|0\rangle + |2\rangle + |3\rangle - |5\rangle), \\ |\xi_B\rangle &= \frac{1}{2}(|0\rangle - |2\rangle + |3\rangle + |5\rangle), \\ |\xi_C\rangle &= \frac{1}{2}(|0\rangle + |1\rangle - |3\rangle + |4\rangle), \\ |\xi_D\rangle &= \frac{1}{2}(|0\rangle - |1\rangle - |3\rangle - |4\rangle), \\ |\xi_E\rangle &= \frac{1}{2}(|1\rangle + |2\rangle - |4\rangle + |5\rangle), \\ |\xi_F\rangle &= \frac{1}{2}(|1\rangle - |2\rangle - |4\rangle - |5\rangle),\end{aligned} \quad (20)$$

are orthogonal states, with $|3\rangle$, $|4\rangle$, and $|5\rangle$ being the basis states in the additional dimensions represented by modes added on Bob's side.

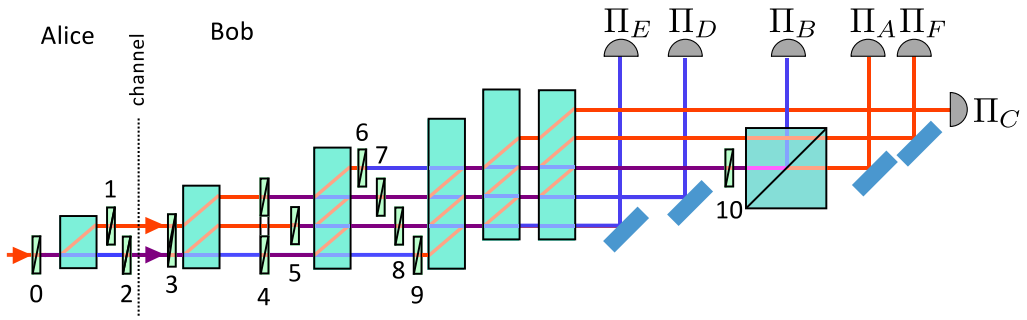

FIG. 3. The experimental setup for the XOT protocol when Bob is honest. The green boxes labeled with black numbers represent half-wave plates (HWPs). The large semitransparent cyan boxes represent beam displacers. Next to HWP10, there is a polarizing beam splitter. Note that HWP4 is ring shaped and that polarization of the central beam is not affected. The detectors are labeled according to the corresponding POVM operators. The settings for Alice's half-wave plates are listed in Table II for when she is honest and in Table III for when she is cheating. The settings for Bob's half-wave plates are HWP3= 0°, HWP4=HWP5=HWP7=HWP8=HWP10= 22.5°, and HWP6=HWP9= 45°. The beams marked in red have horizontal linear polarization and the beams marked in blue have vertical polarization. Purple indicates general polarization states.

A unitary transformation between states $\{|\xi_i\rangle\}_{i=A}^{F}$ and the computational basis $\{|j\rangle\}_{j=0}^{5}$ can be realized by a symmetric beam-splitter network (consisting of six 50:50 beam splitters), which can be further translated into a setup consisting of half-wave plates and a beam displacer that combines spatial and polarization modes of light. The first beam displacer on Bob's side in Fig. 3 just transfers the incoming polarization and spatial modes into three separate paths. The following half-wave plates—"double" HWP4 and HWP5—turned by 22.5° play the role of "beam splitters", mixing the original three modes with the additional three "empty" (vacuum) modes. Each wave plate mixes two polarization modes. Behind the next beam displacer there are two half-wave plates turned by 45°, which just swap horizontal and vertical linear polarizations, and two half-wave plates turned by 22.5°, which represent the other two "beam splitters." The last "beam splitter" of the network is implemented by a half-wave plate turned by 22.5°, followed by a polarizing beam splitter in the right part of the figure.

To prevent the injection of higher-dimensional states into Bob's apparatus (so that Alice only has access to the subspace spanned by her legitimate states), there should be a linear polarizer placed in the upper input port. However, in our proof-of-principle experiment, we omit it in order to simplify the setup.

The measurement results are shown in Table V of Appendix E. This gives the absolute numbers of detector counts, the corresponding relative frequencies, and theoretical probabilities for comparison. The digits in parentheses represent one standard deviation at the final decimal place. The states in Eq. (9) are being prepared with equal probabilities. The average error rate caused by experimental imperfections is 0.01249(8). It is calculated as $(\sum_{i,j\in\mathcal{E}_i} C_{ij})/(\sum_{i,j} C_{ij})$, where i indexes input states, j indexes measurement results, the C_{ij} are measured numbers of counts, and $\mathcal{E}_i$ denotes the sets of erroneous outcomes (outcomes that should not occur).

B. Alice cheating

Bob is honest, so his measurement is the same as in the previous case. To guess which of the three bits Bob will obtain, Alice sends the states $|0\rangle$, $|1\rangle$, or $|2\rangle$. The corresponding angles of the wave plates are listed in Table III.

The measurement results are shown in Table VI of Appendix E. Alice's states are being prepared with equal probabilities. Her average probability of correctly guessing which one of the three bits Bob obtained (i.e., his value of b), estimated from the experiment, is 0.4999(3). It is calculated as $(\sum_{i,j\in\mathcal{C}_i} C_{ij})/(\sum_{i,j} C_{ij})$, where $\mathcal{C}_i$ denotes the sets of correct guesses. The theoretical prediction is 1/2.

TABLE II. The wave-plate angles for Alice's state preparation if Alice is honest. The angle of HWP1 is always zero (it only compensates for path differences). These settings also hold for cheating Bob in the reversed protocol.

	$\|\phi_{00}\rangle$	$\|\phi_{01}\rangle$	$\|\phi_{10}\rangle$	$\|\phi_{11}\rangle$
HWP0	−27.37°	−27.37°	27.37°	27.37°
HWP2	−25.50°	25.50°	25.50°	−25.50°

TABLE III. The angles for wave plates for Alice's state preparation, if Alice is cheating. The angle of HWP1 is always zero.

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$
HWP0	0°	45°	45°
HWP2	0°	45°	0°

C. Bob cheating

Alice is honest, so she sends her states exactly as in the described case above, when both parties were honest. To guess all three bits (equivalently, any two bits), Bob applies the square-root measurement consisting of four positive operator-valued measure (POVM) elements, which are actually the same as that expressed in Eq. (14). This POVM can be implemented by projectors $\{|\xi_i\rangle\langle\xi_i|\}_{i=00}^{11}$ in a four-dimensional Hilbert space spanned by $|0\rangle, |1\rangle, |2\rangle, |3\rangle$, where

$$\begin{aligned}
|\xi_{00}\rangle &= \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right), \\
|\xi_{01}\rangle &= \frac{1}{2}\left(|0\rangle - |1\rangle + |2\rangle - |3\rangle\right), \\
|\xi_{10}\rangle &= \frac{1}{2}\left(|0\rangle + |1\rangle - |2\rangle - |3\rangle\right), \\
|\xi_{11}\rangle &= \frac{1}{2}\left(|0\rangle - |1\rangle - |2\rangle + |3\rangle\right),
\end{aligned} \tag{21}$$

are orthogonal states. The implementation of this projective measurement is shown in Fig. 4. The angles of the wave plates are listed in the figure caption.

The measurement results are shown in Table VII of Appendix E. Alice's states are being prepared with equal probabilities. Bob's average probability of guessing all bits, estimated from the experiment, is 0.7431(3). The theoretical value is 3/4.

D. Reversed protocol—both parties honest

In the reversed protocol, Bob prepares and sends one of the six nonorthogonal qutrit states defined in Eq. (13). These states can be prepared in a similar way as Alice's states were being prepared in the unreversed protocol. The corresponding angles for the wave plates are listed in Table IV.

TABLE IV. The reversed protocol. The wave-plate angles for Bob's state preparation, if Bob is honest. The angle of HWP1 is always zero. $x_2 = x_0 \oplus x_1$.

	$\|\phi_{x_0=0}\rangle$	$\|\phi_{x_0=1}\rangle$	$\|\phi_{x_1=0}\rangle$	$\|\phi_{x_1=1}\rangle$	$\|\phi_{x_2=0}\rangle$	$\|\phi_{x_2=1}\rangle$
HWP0	−22.5°	22.5°	22.5°	−22.5°	45.0°	45.0°
HWP2	0.0°	0.0°	45.0°	45.0°	−22.5°	22.5°

In this case, Alice is the receiver. To learn the bit values, she performs a POVM measurement, the components of which are defined in Eq. (14). We already know how to implement this measurement, because it is exactly the same as the measurement for cheating Bob in the unreversed protocol. So the corresponding higher-dimensional projective measurement consists of the projectors onto the states in Eq. (21). Therefore, the setup for the reversed protocol in the case when both parties are honest is actually the same as the setup for the unreversed protocol when Bob is cheating (see Fig. 4) except that the roles of Alice and Bob are interchanged.

The measurement results are shown in Table VIII of Appendix E. Bob's states are being prepared with equal probabilities. The average error rate caused by experimental imperfections is 0.00428(4).

E. Reversed protocol—Alice cheating

Bob honestly prepares his quantum states but cheating Alice wants to know which bit Bob has actually learned. In this case, Alice's optimal strategy is to use the measurement defined in Eq. (D6). These POVM operators are actually statistical mixtures of the projectors onto the basis states $|0\rangle$, $|1\rangle$, and $|2\rangle$. This means that Alice can make a projective measurement followed by classical postprocessing. For example, if she obtains the result corresponding to $|0\rangle\langle 0|$, she knows that Bob has either the value of bit x_0 or the value of bit x_1, each with 50% probability. The scheme of the setup implementing Alice's measurement if she is

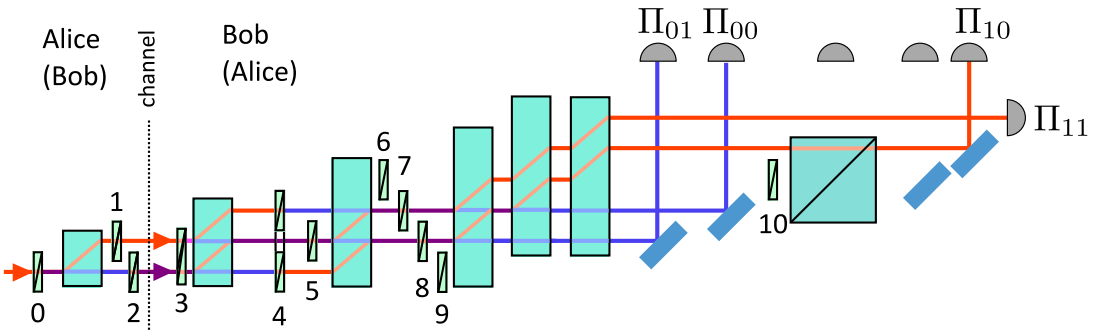

FIG. 4. The experimental setup for the XOT protocol when Bob is cheating. The notation is the same as in Fig. 3. The settings for the receiver's half-wave plates are HWP3 = HWP7 = HWP8 =22.5°, HWP4 =45°, and HWP5= 90°. The same setup is used for the reversed protocol when Alice is honest but in that case, Bob is the sender and Alice is the receiver (names in parentheses). The settings of the sender's half-wave plates for honest Alice in the unreversed protocol, or for cheating Bob in the reversed protocol, are listed in Table II, and for honest Bob in the reversed protocol in Table IV.

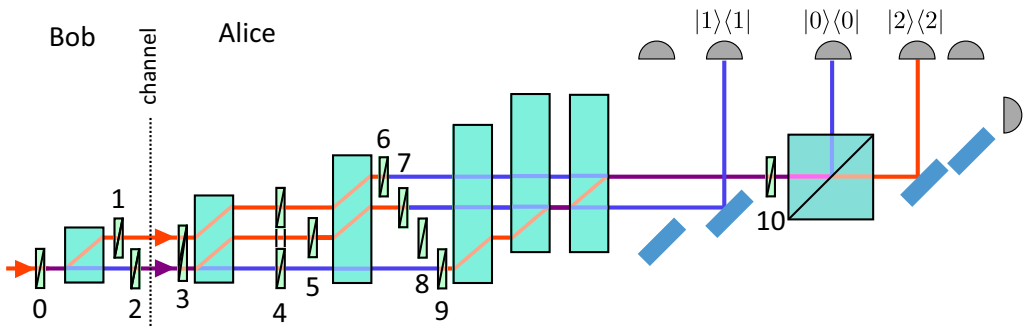

FIG. 5. The experimental setup for the reversed XOT protocol when Alice is cheating. The notation is the same as in Fig. 3. The settings of Alice's half-wave plates are HWP3 = HWP4 = HWP10 = 0°, HWP5 = 90°, and HWP6 = HWP7 = HWP9 = 45°.

cheating is shown in Fig. 5. The angles of the wave plates are listed in the figure caption.

The measurement results are shown in Table IX of Appendix E. Bob's states are being prepared with equal probabilities. The average probability of Alice guessing Bob's b, estimated from the experiment, is 0.4992(2). The theoretical value is $1/2$.

F. Reversed protocol—Bob cheating

In this case, Alice behaves honestly but cheating Bob wants to obtain the values of both x_0 and x_1 (and their XOR). To estimate these values, Bob uses a set of four "fake" states, which are equivalent to the states in Eq. (9). Clearly, the experimental setup, as well as the state preparation and measurement, are the same as that for the unreversed protocol with cheating Bob (see Fig. 4). Therefore, it is not necessary to repeat the measurement because the results have already been obtained. They are shown in Table VII of Appendix E. The average probability of Bob guessing all bits, estimated from the experiment, is 0.7431(3). The theoretical value is $3/4$.

G. Technical description of the setup

We use a heralded single-photon source. The heralding is based on the detection of one photon from a time-correlated pair. Photon pairs are generated using type-II spontaneous parametric down-conversion in a periodically poled potassium titanyl phosphate (KTP) crystal and their wavelength is 810 nm. The photons enter the setup with linear horizontal polarization. Single-photon detection is implemented as coincidence measurements with the trigger signal heralding photon creation. The coincidence window used is 2.5 ns. If more detectors click together with the trigger signal, only one result is randomly selected and counted. However, such situations occur at most once in 2000 measurements.

Each qutrit used in the protocol is represented by a single photon that can occur in a superposition of three optical modes. The protocol requires an interferometric network that allows coupling of these modes with each other and with a vacuum. Our implementation, depicted in Fig. 6, is based on calcite beam displacers, which allow us to construct passively stable interferometers [28]. We use spatial and polarization degrees of freedom to encode the qutrits. This encoding enables us to realize a tunable beam

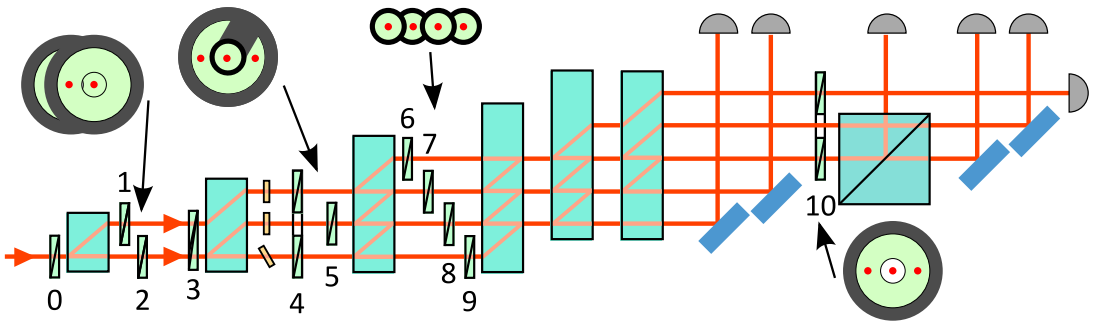

FIG. 6. The detailed scheme of the experimental setup. The green boxes labeled with black numbers represent HWPs. The small orange rectangles are glass plates that serve for phase compensation. The large semitransparent cyan boxes represent beam displacers. Next to HWP10, there is a polarizing beam splitter. Note that HWP1, HWP2, HWP4, and HWP10 are ring shaped and that polarization of the central beam is not affected. The insets show the actual arrangement of the half-wave plates.

splitter simply with a half-wave plate that couples horizontally and vertically polarized optical modes. The calcite beam displacers spatially separate horizontally and vertically polarized components into two parallel beams with 6 mm lateral distance.

Although there are multiple optical paths, only four interferometric phases are important for the tested protocols. To adjust these phases, we use auxiliary wave-plate settings such that the output optical signal is sensitive to the optical phase. The first relative optical phase is set by tilting the second beam displacer using a piezo-stack actuator attached to the prism turntable. Then we adjust the second phase by tilting the third beam displacer. The third phase is set by tilting the glass plate in the bottom arm. Finally, we set the last optical phase by tilting the fourth beam displacer. The phases have to be set in this order due to the sharing of optical paths.

Using strong laser light, we characterize the phase stability of the largest interferometer formed by the outermost optical paths between the first and the fourth beam displacers, which merge at the sixth displacer. We set the optical phase roughly to $\pi/2$, cover the setup with a cardboard box, and monitor the output intensity for 1 h. The observed drift speed is 0.5°/min. The amplitude of fast phase fluctuation is roughly 5° peak to peak.

There are several sources of experimental error. The most significant of them is the unequal fiber-coupling efficiencies at the output of the interferometric network, spanning from 0.75 to 0.85. Furthermore, the efficiencies of the used single-photon detectors are also unequal. The largest relative difference is 0.12. We compensate for these inequalities using detection electronics. The inaccurate retardance of half-wave plates causes the discrepancy between the expected and actual coupling ratios for a given angular position. We try to compensate for this imperfection by slight modifications of the angular positions. Also, we use wave plates to exchange the polarization modes. The imperfect retardance limits the ability to turn the horizontal into vertical polarization. It consequently causes undesired losses and residual coupling in our experiments. Furthermore, the slight variation in the length of the beam displacers causes imperfect overlap of optical beams, reducing the interferometric visibility. The worst visibility that we observe is 0.85. Fortunately, coupling the beams into single-mode optical fibers serves as spatial filtering and restores interferometric visibility. The worst observed visibility of the fiber-coupled signal is 0.99. We also observe that different optical paths suffer from slightly unequal optical losses (the largest difference is 0.02), but we do not directly compensate for this imperfection.

The counts C_{ij} are accumulated during 10-s measurements for each input state. Relative frequencies are calculated as $f_{ij} = C_{ij}/\sum_j C_{ij}$, where i is indexing the input states and j is indexing the measurement results. The shown errors of the relative frequencies are determined using the standard law of error propagation under the assumption that the detection events obey the Poissonian distribution and thus the standard deviations of C_{ij} can be estimated as $\sqrt{C_{ij}}$. The key part of the experiment is a stable optical realization of the required POVM measurements.

VI. CONCLUSIONS

We analyze and realize protocols for quantum XOR oblivious transfer. The protocols are noninteractive, do not require entanglement, and make use of pure symmetric states. We present particular optimal quantum protocols, showing that they outperform classical XOR oblivious transfer protocols, and obtain cheating probabilities for the sender and receiver for general noninteractive symmetric-state protocols. The cheating probabilities for the protocols are the same as for a previous protocol [26], which is interactive and requires entanglement. Noninteractive protocols that do not require entanglement are, however, simpler to implement. In our protocol, Bob obtains Alice's first bit, her second bit, or their XOR at random. Thus, we introduce the concept of semirandom XOT protocols, analogous to the definition of semirandom 1-2 OT protocols given in Ref. [15], proving that a semirandom XOT protocol can be changed into a standard XOT protocol and vice versa by adding classical postprocessing, keeping the cheating probabilities the same.

One can argue that the "quantum advantage" for the presented quantum XOT oblivious transfer protocol is greater than that of the quantum 1-out-of-2 oblivious transfer protocol in Ref. [15]. In addition, the cheating probabilities for the protocol in Ref. [15] are average cheating probabilities for many rounds of oblivious transfer. A sender can cheat with probability 1 in any single round, with negligible probability of being caught, as long as the average cheating probability obeys the bound. For the XOR oblivious transfer protocol that we present, the sender's cheating probability in every single round is bounded by 1/2.

We also introduce the concept of "reversing" a protocol, which means that the sender of the quantum state instead becomes a receiver of quantum states and vice versa, while keeping their roles in the XOT protocol the same. This is useful if one party only has the ability to prepare and send quantum states, while the other party can only measure them. This is frequently the case in quantum communications systems. The "original" and "reversed" protocols can be connected by viewing them in terms of a shared entangled state. Because the two parties do not trust each other in oblivious transfer, or in multiparty computation more generally, unlike for quantum key distribution, the cheating probabilities can be different depending on who prepares the entangled state. For our XOT protocol, however, the cheating probabilities are the same in the unreversed protocol and in its reversed version.

We optically realize both the unreversed and the reversed version of our optimal noninteractive quantum XOT protocol, including Alice's and Bob's optimal cheating strategies. The experiment involves the implementation of the generalized quantum measurements made by the receiver Bob in the unreversed protocol and the sender Alice in the reversed protocol. This is achieved through extending the Hilbert space using an auxiliary basis state, which is coupled to the other basis states using a particular unitary transform. The experimental work involves aligning and stabilizing several concatenated Mach-Zehnder interferometers, which is not trivial. Generalized measurements are still quite rare in quantum communication and quantum cryptographic protocols, which mostly use standard projective quantum measurements. The achieved experimental data match our theoretical results very well, thus demonstrating the feasibility of both protocols.

ACKNOWLEDGMENTS

This work was supported by the United Kingdom Engineering and Physical Sciences Research Council (EPSRC) under Grants No. EP/T001011/1 and No. EP/R513386/1. R.S., N.H., and M.D. acknowledge support by Palacký University under Grants No. IGA-PrF-2021-006 and No. IGA-PrF-2022-005.

APPENDIX A: QUANTUM XOT WITH SYMMETRIC STATES: DETAILS OF DERIVATIONS

1. Conditions involving pairwise overlaps

We first give a number of useful relations. For a set of symmetric pure states, the pairwise overlaps obey

$$\begin{aligned}&\langle\psi_{01}|\psi_{00}\rangle = \langle\psi_{11}|\psi_{01}\rangle = \langle\psi_{10}|\psi_{11}\rangle = \langle\psi_{00}|\psi_{10}\rangle = F,\\ &\langle\psi_{00}|\psi_{11}\rangle = \langle\psi_{01}|\psi_{10}\rangle = G.\end{aligned} \tag{A1}$$

Since $|\psi_{11}\rangle = U^2|\psi_{00}\rangle$ and the eigenvalues of U are the fourth roots of unity, G is always real but F is in general complex. We denote an honest Bob's measurement operators by Π_{0*}, Π_{1*}, Π_{*0}, Π_{*1}, $\Pi_{\text{XOR}=0}$, and $\Pi_{\text{XOR}=1}$ (using different indices than in Sec. III, in order to distinguish these more general measurement operators from the specific ones in Sec. III). Bob should obtain either the first or second bit, or their XOR, each with probability 1/3. The probability of obtaining outcome m is

$$p_m = \langle\psi_{jk}|\,\Pi_m\,|\psi_{jk}\rangle\,,$$

for $m \in \{0*, 1*, *0, *1, \text{XOR}=0, \text{XOR}=1\}$. This probability should be equal to 1/3 when an outcome is possible and otherwise be equal to 0. Moreover, it holds that

$$\begin{aligned}\langle\psi_{01}|\,\Pi_{0*}\,|\psi_{00}\rangle &= \langle\psi_{10}|\,\Pi_{1*}\,|\psi_{11}\rangle =\\ \langle\psi_{00}|\,\Pi_{*0}\,|\psi_{10}\rangle &= \langle\psi_{11}|\,\Pi_{*1}\,|\psi_{01}\rangle = F,\\ \langle\psi_{00}|\,\Pi_{\text{XOR}=0}\,|\psi_{11}\rangle &= \langle\psi_{01}|\,\Pi_{\text{XOR}=1}\,|\psi_{10}\rangle = G.\end{aligned} \tag{A2}$$

The above relations can be obtained by writing $\Pi_{0*} = \sum_k \lambda_k |\lambda_k\rangle\langle\lambda_k|$ in terms of its eigenstates and eigenvalues and similarly for the other measurement operators. It then holds, for example, that

$$0 = \langle\psi_{10}|\,\Pi_{0*}\,|\psi_{10}\rangle = \sum_k \lambda_k |\langle\psi_{10}|\lambda_k\rangle|^2, \tag{A3}$$

meaning that $\langle\psi_{10}|\lambda_k\rangle = 0\ \forall\ k$. Using this and other analogous conditions, we have

$$F = \langle\psi_{01}|\psi_{00}\rangle = \langle\psi_{01}|\sum_m \Pi_m\,|\psi_{00}\rangle = \langle\psi_{01}|\,\Pi_{0*}\,|\psi_{00}\rangle\,. \tag{A4}$$

The other conditions in Eq. (A2) can be obtained analogously. Furthermore, it has to hold that $|F| \le 1/3$ and $|G| \le 1/3$. This is necessary for the states to be distinguishable enough, so that an honest Bob can learn either x_0, x_1, or $x_0 \oplus x_1$ correctly. To show this, define a vector $\mathbf{X}$ with elements $x_k = \sqrt{\lambda_k}\,\langle\psi_{01}|\lambda_k\rangle$ and a vector $\mathbf{Y}$ with elements $y_k = \sqrt{\lambda_k}\,\langle\psi_{00}|\lambda_k\rangle$. Then, $|\mathbf{X}|^2 = |\mathbf{Y}|^2 = 1/3$ and it holds that

$$\begin{aligned}|F|^2 &= |\sum_k \lambda_k\,\langle\psi_{01}|\lambda_k\rangle\,\langle\lambda_k|\psi_{00}\rangle\,|^2 = |\sum_k x_k y_k^*|^2\\ &\le |\mathbf{X}|^2|\mathbf{Y}|^2 = \frac{1}{9}.\end{aligned} \tag{A5}$$

$|G| \le 1/3$ can be proven analogously.

2. Alice's cheating probability when Bob is testing her states

In order to always be able to pass Bob's tests, a dishonest Alice must use an equal superposition of the states that she is supposed to send, entangled with a system that she keeps on her side. That is a state of the form

$$\begin{aligned}|\Psi_{\text{cheat}}\rangle = a\,|0\rangle_A \otimes |\psi_{00}\rangle + b\,|1\rangle_A \otimes |\psi_{01}\rangle\\ + c\,|2\rangle_A \otimes |\psi_{11}\rangle + d\,|3\rangle_A \otimes |\psi_{10}\rangle\,,\end{aligned} \tag{A6}$$

where $|0\rangle_A, |1\rangle_A, |2\rangle_A, |3\rangle_A$ is an orthonormal basis for her kept system and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. If Alice measures her system in this basis, she can always pass any tests that Bob might conduct. It will appear to Bob as if Alice is sending one of the four states that she should send if she is honest.

We set $a = b = c = d = 1/2$, which we conjecture is actually optimal for Alice. Any cheating strategy for Alice will nevertheless give a lower bound on her cheating probability. Honest Bob performs a measurement with measurement operators Π_{0*}, Π_{1*}, Π_{*0}, Π_{*1}, $\Pi_{\mathrm{XOR}=0}$, and $\Pi_{\mathrm{XOR}=1}$ on the system that he receives. Using the conditions in Eq. (A2), we can express the equiprobable states Alice holds, conditioned on Bob's b, as

$$\mu_A^{b=0} = \frac{1}{4}\begin{pmatrix} 1 & 3F & 0 & 0 \\ 3F^* & 1 & 0 & 0 \\ 0 & 0 & 1 & 3F \\ 0 & 0 & 3F^* & 1 \end{pmatrix},$$
$$\mu_A^{b=1} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 3F^* \\ 0 & 1 & 3F & 0 \\ 0 & 3F^* & 1 & 0 \\ 3F & 0 & 0 & 1 \end{pmatrix}, \qquad \text{(A7)}$$
$$\mu_A^{b=2} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 3G & 0 \\ 0 & 1 & 0 & 3G \\ 3G & 0 & 1 & 0 \\ 0 & 3G & 0 & 1 \end{pmatrix},$$

corresponding to Bob obtaining x_0, x_1, or $x_2 = x_0 \oplus x_1$. Here,

$$\mu_A^{b=0} = \frac{\mathrm{Tr}_B\left[(\Pi_{0*}+\Pi_{1*})^{1/2}\,|\Psi_{\mathrm{cheat}}\rangle\langle\Psi_{\mathrm{cheat}}|\,(\Pi_{0*}+\Pi_{1*})^{1/2}\right]}{p_{0*}+p_{1*}},$$

where

$$p_{0*}+p_{1*} = \mathrm{Tr}[|\Psi_{\mathrm{cheat}}\rangle\langle\Psi_{\mathrm{cheat}}|\,(\Pi_{0*}+\Pi_{1*})] = \frac{1}{3}$$

and analogously for $b = 1$ and $b = 2$. These states are mirror symmetric, meaning that the unitary transformation that takes $|0\rangle \to |3\rangle$, $|3\rangle \to |2\rangle$, $|2\rangle \to |1\rangle$, and $|1\rangle \to |0\rangle$, takes $\mu_A^{b=0}$ to $\mu_A^{b=1}$ and vice versa, and keeps $\mu_A^{b=2}$ unchanged. The minimum-error measurement is known for some sets of mirror-symmetric states [29,30] but this is not one of them. Alice's minimum-error measurement can nevertheless be found by making a basis transform using a unitary transform U proportional to a 4×4 Hadamard-Walsh matrix:

$$U = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \qquad \text{(A8)}$$

If we interpret the four basis states as two-qubit states so that $|0\rangle \equiv |00\rangle$, $|1\rangle \equiv |01\rangle$, $|2\rangle \equiv |10\rangle$, and $|3\rangle \equiv |11\rangle$, this is the same as writing the density matrices in the $|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle$ basis, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The density matrices in Eq. (A7) then become

$$\mu_A^{b=0} = \frac{1}{4}\begin{pmatrix} 1+3\,\mathrm{Re}\,F & -3i\,\mathrm{Im}\,F & 0 & 0 \\ 3i\,\mathrm{Im}\,F & 1-3\,\mathrm{Re}\,F & 0 & 0 \\ 0 & 0 & 1+3\,\mathrm{Re}\,F & -3i\,\mathrm{Im}\,F \\ 0 & 0 & 3i\,\mathrm{Im}\,F & 1-3\,\mathrm{Re}\,F \end{pmatrix},$$
$$\mu_A^{b=1} = \frac{1}{4}\begin{pmatrix} 1+3\,\mathrm{Re}\,F & 3i\,\mathrm{Im}\,F & 0 & 0 \\ -3i\,\mathrm{Im}\,F & 1-3\,\mathrm{Re}\,F & 0 & 0 \\ 0 & 0 & 1-3\,\mathrm{Re}\,F & -3i\,\mathrm{Im}\,F \\ 0 & 0 & 3i\,\mathrm{Im}\,F & 1+3\,\mathrm{Re}\,F \end{pmatrix}, \qquad \text{(A9)}$$
$$\mu_A^{b=2} = \frac{1}{4}\begin{pmatrix} 1+3G & 0 & 0 & 0 \\ 0 & 1+3G & 0 & 0 \\ 0 & 0 & 1-3G & 0 \\ 0 & 0 & 0 & 1-3G \end{pmatrix}.$$

All three density matrices are block diagonal. This means that the minimum-error measurement can be performed by first projecting on the subspaces corresponding to each block, which is the same as measuring the first qubit in the $|+\rangle, |-\rangle$ basis. Depending on the outcome, one then distinguishes between the resulting three density matrices in that subspace. In each subspace, $\mu_A^{b=2}$ is proportional to an identity matrix. This means that no measurement will tell Alice anything more about the likelihood that her state was $\mu_A^{b=2}$ other than what she already knows. The optimal measurement in each subspace is then the measurement that optimally distinguishes between $\mu_A^{b=0}$ and

$\mu_A^{b=1}$. Depending on the outcome, Alice's best guess might still be $b = 2$.

To summarize, the measurement that distinguishes between $\mu_A^{b=0}, \mu_A^{b=1}$, and $\mu_A^{b=2}$ with minimum error, and therefore maximizes Alice's cheating probability, is a projection on the states $|+R\rangle$, $|+L\rangle$, $|-+\rangle$, and $|--\rangle$, where $|R\rangle = (|0\rangle + i\,|1\rangle)/\sqrt{2}$ and $|L\rangle = (|0\rangle - i\,|1\rangle)/\sqrt{2}$. The probabilities for the different outcomes, conditioned on what density matrix Alice holds, are

$$\begin{aligned}
p(+,R|\mu_A^{b=0}) &= p(+,L|\mu_A^{b=1}) = \frac{1}{4}(1 + 3\ \mathrm{Im}\ F),\\
p(+,L|\mu_A^{b=0}) &= p(+,R|\mu_A^{b=1}) = \frac{1}{4}(1 - 3\ \mathrm{Im}\ F),\\
p(+,L|\mu_A^{b=2}) &= p(+,R|\mu_A^{b=2}) = \frac{1}{4}(1 + 3G),\\
p(-,+|\mu_A^{b=0}) &= p(-,-|\mu_A^{b=1}) = \frac{1}{4}(1 + 3\ \mathrm{Re}\ F),\\
p(-,-|\mu_A^{b=0}) &= p(-,+|\mu_A^{b=1}) = \frac{1}{4}(1 - 3\ \mathrm{Re}\ F),\\
p(-,+|\mu_A^{b=2}) &= p(-,-|\mu_A^{b=2}) = \frac{1}{4}(1 - 3G).
\end{aligned} \tag{A10}$$

Given one of the four outcomes, Alice chooses the most likely value of b. Her cheating probability is then bounded as

$$A_{\mathrm{OT}} \geq \begin{cases} \frac{1}{3} + \frac{1}{2}|\mathrm{Im}\ F| + \frac{1}{2}\max(|\mathrm{Re}\ F|, |G|), & \text{if } G \leq 0,\\ \frac{1}{3} + \frac{1}{2}|\mathrm{Re}\ F| + \frac{1}{2}\max(|\mathrm{Im}\ F|, |G|), & \text{if } G > 0, \end{cases} \tag{A11}$$

as given in Eq. (3).

3. Alice's cheating probability when Bob is not testing her states

It is optimal for Alice to send Bob the pure state, within the subspace spanned by the states that she is supposed to send him, for which Bob's probability of obtaining either $b = 0$, $b = 1$, or $b = 2$ is maximized. Alice's state can be written

$$|\Psi_{\mathrm{cheat}}\rangle = \alpha\,|\psi_{00}\rangle + \beta\,|\psi_{01}\rangle + \gamma\,|\psi_{11}\rangle + \delta\,|\psi_{10}\rangle\,, \tag{A12}$$

where α, β, γ, and δ are complex coefficients, chosen so that the state is normalized. Bob's probabilities of obtaining $b = 0, b = 1$, and $b = 2$ are

$$\begin{aligned}
p(b=0) &= \langle\Psi_{\mathrm{cheat}}|\,\Pi_{0*} + \Pi_{1*}\,|\Psi_{\mathrm{cheat}}\rangle\,,\\
p(b=1) &= \langle\Psi_{\mathrm{cheat}}|\,\Pi_{*0} + \Pi_{*1}\,|\Psi_{\mathrm{cheat}}\rangle\,,\\
p(b=2) &= \langle\Psi_{\mathrm{cheat}}|\,\Pi_{\mathrm{XOR}=0} + \Pi_{\mathrm{XOR}=1}\,|\Psi_{\mathrm{cheat}}\rangle\,,
\end{aligned} \tag{A13}$$

which, using the conditions in Eq. (A2), can be written

$$\begin{aligned}
p(b=0) &= \frac{1}{3}(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2)\\
&\quad + (\alpha\beta^* + \gamma\delta^*)F + (\alpha^*\beta + \gamma^*\delta)F^*,\\
p(b=1) &= \frac{1}{3}(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2)\\
&\quad + (\alpha^*\delta + \beta\gamma^*)F + (\alpha\delta^* + \beta^*\gamma)F^*,\\
p(b=2) &= \frac{1}{3}(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2)\\
&\quad + (\alpha^*\gamma + \beta^*\delta + \alpha\gamma^* + \beta\delta^*)G.
\end{aligned} \tag{A14}$$

Alice should choose α, β, γ, and δ so as to maximize one of these probabilities. Normalization means that $p(b = 0) + p(b = 1) + p(b = 2) = 1$.

Bob's probabilities in Eq. (A14) can also be written as

$$\begin{aligned}
p(b=0) &= \left(\frac{1}{3} - |F|\right)\left(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2\right)\\
&\quad + |F|\left(|\alpha e^{i\theta_F} + \beta|^2 + |\gamma e^{i\theta_F} + \delta|^2\right),\\
p(b=1) &= \left(\frac{1}{3} - |F|\right)\left(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2\right)\\
&\quad + |F|\left(|\alpha e^{-i\theta_F} + \delta|^2 + |\beta + \gamma e^{-i\theta_F}|^2\right),\\
p(b=2) &= \left(\frac{1}{3} - |G|\right)\left(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2\right)\\
&\quad + |G|\left(|\alpha \pm \gamma|^2 + |\beta \pm \delta|^2\right),
\end{aligned} \tag{A15}$$

where in the expression for $p(b = 2)$, we have "+" if $G > 0$ and "−" if $G < 0$. From the above expressions, we see that if $|F| = |G| = 1/3$, then Alice can cheat perfectly unless $F = \pm 1/3$ and $G = -1/3$, or $F = \pm i/3$ and $G = 1/3$. Unless one of these conditions hold, Alice can make $p(b = 2)$ and either $p(b = 0)$ or $p(b = 1)$ equal to zero, while the remaining probability is equal to 1. To make $p(b = 1) = p(b = 2) = 0$ when $G = 1/3$, for example, Alice chooses $\alpha = -\delta e^{i\theta_F} = \beta e^{i\theta_F} = -\gamma$. Then $p(b = 0) = 1$, unless it holds that $e^{2i\theta_F} = -1$, which is the case for $F = \pm i/3$. As we show, for $F = \pm 1/3$, $G = -1/3$ or $F = \pm i/3$, $G = 1/3$, Alice's cheating probability is equal to $1/2$ whether Bob tests the state that she sends him or not. We have already seen that these choices of phases for F and G, when $|F| = |G| = 1/3$, also minimize Bob's cheating probability in Eq. (2). We now find that they are the optimal—or even the only sensible—choices more generally whenever $|F| = |G| = 1/3$, when Bob does not test Alice's state (since otherwise Alice can cheat with probability 1).

We now derive Alice's cheating probabilities as a function of F and G. Bob's probabilities $p(b = 0)$, $p(b = 1)$,

and $p(b=2)$ can be written in bilinear form as

$$p(b=i) = (\alpha^*, \beta^*, \gamma^*, \delta^*) M_i (\alpha, \beta, \gamma, \delta)^T, \tag{A16}$$

where $i = 0, 1, 2$, and the matrices M_0, M_1, and M_2 are given by

$$M_0 = \begin{pmatrix} 1/3 & F^* & 0 & 0 \\ F & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & F^* \\ 0 & 0 & F & 1/3 \end{pmatrix},$$
$$M_1 = \begin{pmatrix} 1/3 & 0 & 0 & F \\ 0 & 1/3 & F^* & 0 \\ 0 & F & 1/3 & 0 \\ F^* & 0 & 0 & 1/3 \end{pmatrix}, \tag{A17}$$
$$M_2 = \begin{pmatrix} 1/3 & 0 & G & 0 \\ 0 & 1/3 & 0 & G \\ G & 0 & 1/3 & 0 \\ 0 & G & 0 & 1/3 \end{pmatrix}.$$

The normalization condition is then written

$$(\alpha^*, \beta^*, \gamma^*, \delta^*)(M_0 + M_1 + M_2)(\alpha, \beta, \gamma, \delta)^T = 1 \tag{A18}$$

and can be viewed as an ellipsoid in a four-dimensional complex space. The conditions

$$p(b=0) = C_0,\ p(b=1) = C_1,\ p(b=2) = C_2, \tag{A19}$$

where C_0, C_1, and C_2 are some real constants, similarly define ellipsoids in a complex four-dimensional space.

To maximize $p(b=i)$ subject to the normalization constraint in Eq. (A18) is then equivalent to finding the largest C_i for which the ellipsoid for $p(b=i)$ still shares points with the normalization ellipsoid defined by Eq. (A18). The ellipsoids will then be tangent to each other.

In order to find the corresponding maximal values of C_0, C_1, and C_2, we first express all ellipsoids in the basis corresponding to the major axes of the ellipsoid for $M_0 + M_1 + M_2$. Then, we rescale these axes so that the normalization ellipsoid becomes a sphere with radius 1 in four-dimensional complex space (the lengths of all major axes are the same). This will "squash" the ellipsoids corresponding to M_0, M_1, and M_2 but they remain ellipsoids. The largest possible value for C_i will then be obtained when the normalization ellipsoid—now a sphere—is just contained inside the transformed ellipsoid corresponding to M_i, with the ellipsoid tangent to the sphere. This will be the case when the shortest major axis of the transformed ellipsoid for M_i has length 1 (the same length as the radius of the normalization sphere).

The major axes of an ellipsoid can be found from the eigenvectors of the corresponding matrix and the lengths of the major axes can be found from the respective eigenvalues. In the eigenbasis of the corresponding matrix, the equation for an ellipsoid can be written

$$\sum_i \lambda_i |x_i|^2 = C, \tag{A20}$$

where the λ_i are the eigenvalues of the corresponding matrix, the x_i are the coordinates expressed in the eigenbasis, and C is a constant. The lengths of the major axes of this ellipsoid are given by $\sqrt{C/\lambda_i}$. The shortest major axis corresponds to the largest $\lambda_i = \lambda_{\max}$. If the shortest major axis has length 1, then the largest possible value of C is equal to $\lambda_{\max}$.

We therefore need to find the eigenvalues of the transformed M_0, M_1, and M_2 for the corresponding squashed ellipsoids. The largest possible $p(b=i)$ Alice can obtain is then given by the largest of these eigenvalues. The matrix $M_0 + M_1 + M_2$ is circulant and hence its eigenvectors are the "finite Fourier transform (FFT) vectors"

$$|\lambda_0\rangle = \frac{1}{2}(1,1,1,1)^T, \quad |\lambda_1\rangle = \frac{1}{2}(1,i,-1,-i)^T,$$
$$|\lambda_2\rangle = \frac{1}{2}(1,-1,1,-1)^T, \quad |\lambda_3\rangle = \frac{1}{2}(1,-i,-1,i)^T. \tag{A21}$$

The corresponding eigenvalues are

$$\lambda_0 = 1 + G + 2\mathrm{Re}\, F, \quad \lambda_1 = 1 - G + 2\mathrm{Im}\, F,$$
$$\lambda_2 = 1 + G - 2\mathrm{Re}\, F, \quad \lambda_3 = 1 - G - 2\mathrm{Im}\, F. \tag{A22}$$

We now define a matrix V, with columns given by the FFT vectors in Eq. (A21), and a diagonal matrix

$$D_{\mathrm{sq}} = \mathrm{diag}(\sqrt{\lambda_0}, \sqrt{\lambda_1}, \sqrt{\lambda_2}, \sqrt{\lambda_3}). \tag{A23}$$

It then holds that

$$D_{\mathrm{sq}}^{-1} V^\dagger (M_0 + M_1 + M_2) V D_{\mathrm{sq}}^{-1} = \mathrm{diag}(1,1,1,1), \tag{A24}$$

that is, a 4×4 identity matrix. This transformation corresponds to writing the normalization ellipsoid in scaled coordinates where it corresponds to a sphere. In these same coordinates, the equation for the ellipsoid corresponding to a matrix M is

$$(\tilde{\alpha}^*, \tilde{\beta}^*, \tilde{\gamma}^*, \tilde{\delta}^*) D_{\mathrm{sq}}^{-1} V^\dagger M V D_{\mathrm{sq}}^{-1} (\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}, \tilde{\delta})^T = C, \tag{A25}$$

where C is a constant and

$$(\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}, \tilde{\delta})^T = D_{\mathrm{sq}} V^\dagger (\alpha, \beta, \gamma, \delta)^T \tag{A26}$$

are the coordinates in the transformed basis.

The matrix M_2 is diagonal in the same basis as $M_0 + M_1 + M_2$ and the calculation is simpler in this case. The eigenvalues of the transformed matrix $D_{\rm sq}^{-1} V^\dagger M_2 V D_{\rm sq}^{-1}$ are

$$\tilde{\lambda}_{20} = \frac{1/3 + G}{1 + G + 2\mathrm{Re}\, F}, \quad \tilde{\lambda}_{21} = \frac{1/3 - G}{1 - G + 2\mathrm{Im}\, F},$$
$$\tilde{\lambda}_{22} = \frac{1/3 + G}{1 + G - 2\mathrm{Re}\, F}, \quad \tilde{\lambda}_{23} = \frac{1/3 - G}{1 - G - 2\mathrm{Im}\, F}, \tag{A27}$$

which are simply the eigenvalues of M_2 divided by the corresponding eigenvalues of $M_0 + M_1 + M_2$. It follows that the largest $p(b = 2)$ that Alice can achieve is

$$p(b = 2)_{\max} = \begin{cases} \frac{1/3+G}{1+G-2|\mathrm{Re}\, F|}, & \text{if } G \geq \frac{|\mathrm{Im}\, F| - |\mathrm{Re}\, F|}{2 - 3|\mathrm{Re}\, F| - 3|\mathrm{Im}\, F|}, \\ \frac{1/3-G}{1-G-2|\mathrm{Im}\, F|}, & \text{if } G < \frac{|\mathrm{Im}\, F| - |\mathrm{Re}\, F|}{2 - 3|\mathrm{Re}\, F| - 3|\mathrm{Im}\, F|}. \end{cases} \tag{A28}$$

The matrices $V^\dagger M_0 V$ and $V^\dagger M_1 V$ are given by

$$V^\dagger M_0 V = \begin{pmatrix} \frac{1}{3} + \mathrm{Re}\, F & 0 & i\mathrm{Im}\, F & 0 \\ 0 & \frac{1}{3} + \mathrm{Im}\, F & 0 & -i\mathrm{Re}\, F \\ -i\mathrm{Im}\, F & 0 & \frac{1}{3} - \mathrm{Re}\, F & 0 \\ 0 & i\mathrm{Re}\, F & 0 & \frac{1}{3} - \mathrm{Im}\, F \end{pmatrix},$$
$$V^\dagger M_1 V = \begin{pmatrix} \frac{1}{3} + \mathrm{Re}\, F & 0 & -i\mathrm{Im}\, F & 0 \\ 0 & \frac{1}{3} + \mathrm{Im}\, F & 0 & i\mathrm{Re}\, F \\ i\mathrm{Im}\, F & 0 & \frac{1}{3} - \mathrm{Re}\, F & 0 \\ 0 & -i\mathrm{Re}\, F & 0 & \frac{1}{3} - \mathrm{Im}\, F \end{pmatrix}, \tag{A29}$$

from which the matrices $D_{\rm sq}^{-1} V^\dagger M_0 V D_{\rm sq}^{-1}$ and $D_{\rm sq}^{-1} V^\dagger M_1 V D_{\rm sq}^{-1}$ can be obtained by dividing the element in position (j, k) by $\sqrt{\lambda_j \lambda_k}$. Both matrices are block diagonal, which can be seen more readily if permuting, e.g., the middle two rows and columns. The eigenvalues of $D_{\rm sq}^{-1} V^\dagger M_0 V D_{\rm sq}^{-1}$ are given by

$$\tilde{\lambda}_{00/02} = \frac{1}{(1+G)^2 - 4(\mathrm{Re}\, F)^2} \left[\frac{1}{3}(1+G) - 2(\mathrm{Re}\, F)^2 \pm \sqrt{\left(\frac{1}{3} + G\right)^2 (\mathrm{Re}\, F)^2 + [(1+G)^2 - 4(\mathrm{Re}\, F)^2](\mathrm{Im}\, F)^2} \right],$$
$$\tilde{\lambda}_{01/03} = \frac{1}{(1-G)^2 - 4(\mathrm{Im}\, F)^2} \left[\frac{1}{3}(1-G) - 2(\mathrm{Im}\, F)^2 \pm \sqrt{\left(\frac{1}{3} - G\right)^2 (\mathrm{Im}\, F)^2 + [(1-G)^2 - 4(\mathrm{Im}\, F)^2](\mathrm{Re}\, F)^2} \right], \tag{A30}$$

where the plus sign is chosen for $\tilde{\lambda}_{00}$ and $\tilde{\lambda}_{01}$ and the minus sign for $\tilde{\lambda}_{02}$ and $\tilde{\lambda}_{03}$. Clearly, $\tilde{\lambda}_{00}$ and $\tilde{\lambda}_{01}$ are the larger pair of eigenvalues and one of these will give the largest probability that Alice can achieve for $p(b = 0)$. The eigenvalues for $D_{\rm sq}^{-1} V^\dagger M_1 V D_{\rm sq}^{-1}$ are identical and hence Alice's cheating probability for $b = 1$ is the same as for $b = 0$:

$$p(b = 0)_{\max} = p(b = 1)_{\max} = \max(\tilde{\lambda}_{00}, \tilde{\lambda}_{01}). \tag{A31}$$

Alice's overall cheating probability is the larger of $p(b = 0)_{\max} = p(b = 1)_{\max}$ and $p(b = 2)_{\max}$.

APPENDIX B: EQUIVALENCE BETWEEN SEMIRANDOM XOT AND STANDARD XOT

Implementation of a semirandom XOT protocol with cheating probabilities $A_{\rm OT}$ and $B_{\rm OT}$ allows us to realize a standard XOT protocol with the same cheating probabilities, when adding classical postprocessing. We now show that this holds true, using similar arguments as in Refs. [15,21], where it has been shown that the variants of random, semirandom, and standard 1-2 OT are equivalent. A random version of 1-2 OT has also already been previously considered in Ref. [31].

Proposition 1. A semirandom XOT protocol with cheating probabilities $A_{\rm OT}$ and $B_{\rm OT}$ is equivalent to having a standard XOT protocol with the same cheating probabilities.

Proof. We examine both directions, i.e., constructing a semirandom XOT from a standard XOT protocol and constructing a standard XOT protocol from a semirandom XOT protocol; i.e., the situation in which the parties possess the means to implement standard XOT but both of them instead wish to implement semirandom XOT or vice versa.

Case 1. Let P be a standard XOT protocol with cheating probabilities $A_{\rm OT}(P)$ and $B_{\rm OT}(P)$. We can construct a semirandom XOT protocol Q with the same cheating probabilities in the following way:

(1) Alice picks $x_0, x_1 \in \{0, 1\}$ uniformly at random. Bob generates $b \in \{0, 1, 2\}$ uniformly at random (in such a way that he no longer actively chooses b).
(2) Alice and Bob perform the XOT protocol P where Alice inputs x_0, x_1, and $x_2 = x_0 \oplus x_1$ and Bob inputs b. Let y be Bob's output.

(3) Alice and Bob abort in Q if and only if they abort in P. Otherwise, the outputs of protocol Q are (b, y) for Bob.

Evidently, Q implements semirandom XOT if both parties follow the protocol. Furthermore, because of the way in which Q is constructed, Alice can cheat in Q if and only if she can cheat in P, and the same for Bob cheating. The cheating probabilities for Alice and Bob are therefore equal in P and Q, $A_{\mathrm{OT}}(Q) = A_{\mathrm{OT}}(P)$, and $B_{\mathrm{OT}}(Q) = B_{\mathrm{OT}}(P)$.

Case 2. Let P be a semirandom XOT protocol with cheating probabilities $A_{\mathrm{OT}}(P)$ and $B_{\mathrm{OT}}(P)$. We can construct a standard XOT protocol Q with the same cheating probabilities in the following way:

(1) Alice has inputs X_0 and X_1, with $X_2 = X_0 \oplus X_1$, and Bob has input $B \in \{0, 1, 2\}$.
(2) Alice and Bob perform the semirandom XOT protocol P where Alice inputs x_0 and x_1, with $x_2 = x_0 \oplus x_1$, whereby she chooses $x_0, x_1 \in \{0, 1\}$ uniformly at random. Let (b, y) be Bob's outputs.
(3) Bob sends $r = (b + B + B) \bmod 3$ to Alice. Let $x'_c = x_{(c+r) \bmod 3}$ for $c \in \{0, 1, 2\}$.
(4) Alice sends (s_0, s_1) to Bob, whereby $s_c = x'_c \oplus X_c$ for $c \in \{0, 1\}$ and $s_2 = s_0 \oplus s_1$. Let $y' = y \oplus s_B$.
(5) Alice and Bob abort in Q if and only if they abort in P. Otherwise, the output of protocol Q is y' for Bob.

If Alice and Bob are honest, then $y = x_b$. Note that $x'_B = x_{(B+r) \bmod 3} = x_{(B+b+B+B) \bmod 3} = x_b$. Hence,

$$y' = y \oplus s_B = x_b \oplus s_B = x'_B \oplus x'_B \oplus X_B = X_B,$$

i.e., y' is indeed equal to X_B. This also holds for $B = 2$, since

$$\begin{aligned} s_2 &= s_0 \oplus s_1 = x'_0 \oplus X_0 \oplus x'_1 \oplus X_1 \\ &= x_0 \oplus x_1 \oplus X_0 \oplus X_1 = x_2 \oplus X_2 = x'_2 \oplus X_2. \end{aligned}$$

With respect to the classical postprocessing described in steps 3 and 4 and security against Alice and Bob, we can conclude the following:

(a) If Alice is honest, she knows r but has no information about b. From $r = (b + B + B) \bmod 3$, she can deduce that $2B = (r - b) \bmod 3$ but she cannot obtain any information about B from this. Hence, the classical postprocessing does not give an honest Alice any more information about which bit Bob has obtained.
(b) If Alice is dishonest, she can correctly guess b with probability $A_{\mathrm{OT}}(P)$. She knows r. Since $2B = (r - b) \bmod 3$, guessing $2B$—or, equivalently, guessing B—is equivalent to guessing b. Therefore, $A_{\mathrm{OT}}(Q) = A_{\mathrm{OT}}(P)$.
(c) If Bob is honest, he knows (s_0, s_1), $s_2 = s_0 \oplus s_1$, and r but has no information about $x_{(b+1) \bmod 3}$ and $x_{(b+2) \bmod 3}$. He cannot learn anything about the other two of Alice's bits, $X_{(B+1) \bmod 3}$ and $X_{(B+2) \bmod 3}$, since

$$\begin{aligned} X_{(B+1) \bmod 3} &= x'_{(B+1) \bmod 3} \oplus s_{(B+1) \bmod 3} \\ &= x_{(B+1+r) \bmod 3} \oplus s_{(B+1) \bmod 3} \\ &= x_{(b+1) \bmod 3} \oplus s_{(B+1) \bmod 3}, \\ X_{(B+2) \bmod 3} &= x'_{(B+2) \bmod 3} \oplus s_{(B+2) \bmod 3} \\ &= x_{(B+2+r) \bmod 3} \oplus s_{(B+2) \bmod 3} \\ &= x_{(b+2) \bmod 3} \oplus s_{(B+2) \bmod 3}. \end{aligned}$$

Hence, the classical postprocessing does not give an honest Bob any more information about the other two bits that Alice has sent.
(d) If Bob is dishonest, he can guess $x_{(b+1) \bmod 3}$ and $x_{(b+2) \bmod 3}$ with probability $B_{\mathrm{OT}}(P)$. He knows (s_0, s_1), $s_2 = s_0 \oplus s_1$, and r. We have $s_c = x'_c \oplus X_c = x_{(c+r) \bmod 3} \oplus X_c$ for $c \in \{0, 1, 2\}$. Thus, $X_c = x_{(c+r) \bmod 3} \oplus s_c$ and, for Bob, guessing (X_0, X_1, X_2) is equivalent to guessing (x_0, x_1, x_2). Therefore, $B_{\mathrm{OT}}(Q) = B_{\mathrm{OT}}(P)$.

■

In the classical postprocessing given above, Alice needs to define her actual bit values as the bits X_0 and X_1, with $X_2 = X_0 \oplus X_1$. The bits x_0, x_1, and $x_2 = x_0 \oplus x_1$ used in the semirandom XOT protocol, on the other hand, are "dummy" values that she chooses uniformly at random. The value of r will tell Alice how to permute the bits x'_c before computing and sending (s_0, s_1), so that Bob can learn the bit X_B that he wants to learn. For example, if $r = 0$, then $b = B$ and the order is fine, so Alice needs to do nothing before computing and sending (s_0, s_1). If $r = 1$, then $b \neq B$ and Alice needs to shift the bits one place to the left, i.e., (x'_1, x'_2, x'_0), before computing and sending (s_0, s_1), so that $s_0 = x'_1 \oplus X_0$ and $s_1 = x'_2 \oplus X_1$. Lastly, if $r = 2$, then $b \neq B$ as well and Alice needs to shift the bits one place to the right, i.e., (x'_2, x'_0, x'_1), before computing and sending (s_0, s_1), so that $s_0 = x'_2 \oplus X_0$ and $s_1 = x'_0 \oplus X_1$. In all these cases, it holds that $s_2 = s_0 \oplus s_1$ and the respective changes due to the order of the x'_c, for $c \in \{0, 1, 2\}$, follow. The value of s_B will in turn tell Bob what to do with the value of y, so that he can learn his chosen bit. If $s_B = 0$, then he keeps the value as it is, and if $s_B = 1$, then he flips the bit value.

As mentioned in Sec. IV, classical postprocessing can also be added to the reversed XOT protocol. In this way, it is possible for Alice to choose which bit values she wants to obtain. The postprocessing is straightforward and involves only classical communication from Alice to Bob.

For brevity, we outline it without full formal proofs. Suppose that Alice has obtained the two bits (x_0, x_1) from the reversed XOT protocol but her desired bits are (X_0, X_1). If either x_0 or x_1 is not the bit value that she wants, she needs to ask Bob to flip the corresponding bit value, if he holds it. This obviously gives Bob no more information about Alice's bit values X_0 and X_1 than what he already has about x_0 and x_1 and also gives Alice no more information about what Bob has learnt. Defining $t_c = x_c \oplus X_c$ for $c \in \{0, 1, 2\}$, Alice sends (t_0, t_1) to Bob (it holds that $t_2 = x_2 \oplus X_2 = t_0 \oplus t_1$). From the reversed XOT protocol, Bob holds the values of b and bit x_b, and calculates $X_b = x_b \oplus t_b$ as his final bit value. Since Bob does not know $x_{(b+1) \bmod 3}$ and $x_{(b+2) \bmod 3}$, $t_{(b+1) \bmod 3}$ and $t_{(b+2) \bmod 3}$ do not help him at all to learn about $X_{(b+1) \bmod 3}$ or $X_{(b+2) \bmod 3}$. He can correctly guess $X_{(b+1) \bmod 3}$ or $X_{(b+2) \bmod 3}$ with the same probability as he can guess $x_{(b+1) \bmod 3}$ or $x_{(b+2) \bmod 3}$. Thus, this classical postprocessing does not increase Bob's cheating probability. It also does not increase Alice's cheating probability, since she receives no communication from Bob during the postprocessing.

APPENDIX C: REWORKING AN INTERACTIVE XOT PROTOCOL INTO A NONINTERACTIVE PROTOCOL

Starting with the interactive XOR oblivious transfer protocol defined as protocol (3) by Kundu *et al.* [26], which uses entangled states, we show how to rework it into a noninteractive XOT protocol that requires no entanglement. In protocol (3), the sender Alice has two input bits, x_0 and x_1, and the receiver Bob prepares one of three possible entangled two-qutrit states $|\psi_b^+\rangle$,

$$\begin{aligned} |\psi_0^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |22\rangle), \\ |\psi_1^+\rangle &= \frac{1}{\sqrt{2}}(|11\rangle + |22\rangle), \\ |\psi_2^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \end{aligned} \tag{C1}$$

depending on his randomly chosen input $b \in \{0, 1, 2\}$, which specifies whether he will learn the first bit x_0, the second bit x_1, or their XOR $x_2 = x_0 \oplus x_1$. Bob then sends one of the qutrits to the sender Alice, who performs a unitary operation

$$U_{(x_0,x_1)} = (-1)^{x_0} |0\rangle\langle 0| + (-1)^{x_1} |1\rangle\langle 1| + |2\rangle\langle 2| \tag{C2}$$

on it, depending on her randomly chosen input bits (x_0, x_1), before sending it back to Bob. Finally, Bob performs the two-outcome measurement $\{|\psi_b^+\rangle\langle\psi_b^+|, \mathbf{1} - |\psi_b^+\rangle\langle\psi_b^+|\}$ and obtains either x_0, x_1, or x_2, depending on his previous choice of b.

We can rework this interactive protocol into a noninteractive protocol, with only one quantum state transmission between Alice and Bob. That this is possible without affecting the cheating probabilities for Alice and Bob is far from evident but it turns out that the cheating probabilities do remain unchanged in this particular case. First, instead of preparing one of the three states that he prepares in protocol (3), Bob could instead prepare the entangled state

$$\begin{aligned} \frac{1}{\sqrt{6}}\big[&(|00\rangle + |22\rangle) \otimes |0\rangle + (|11\rangle + |22\rangle) \otimes |1\rangle \\ &+ (|00\rangle + |11\rangle) \otimes |2\rangle\big]. \end{aligned} \tag{C3}$$

If Bob measures the last qutrit in the $\{|0\rangle, |1\rangle, |2\rangle\}$ basis, he effectively prepares one of the three states in protocol (3), with probability $1/3$ each. The only difference is that his choice of b is now determined by his measurement outcome, rather than being an active choice for Bob. If starting with the state in Eq. (C3), he can also just as well delay his measurement of the final qutrit to the end of the protocol. As we show, classical postprocessing can be used to allow Bob to nevertheless make an active (but random from Alice's point of view) choice of b.

Whether he has measured the final qutrit or not, Bob could then send one of the two first qutrits to Alice. If Alice applies her unitary operation to one of the first two qutrits, then, depending on the values of x_0 and x_1, the overall state becomes

$$\begin{aligned} |\phi_{x_0x_1}\rangle = \frac{1}{\sqrt{6}}\big[&\big((-1)^{x_0}|00\rangle + |22\rangle\big) \otimes |0\rangle \\ &+ \big((-1)^{x_1}|11\rangle + |22\rangle\big) \otimes |1\rangle \\ &+ \big((-1)^{x_0}|00\rangle + (-1)^{x_1}|11\rangle\big) \otimes |2\rangle\big]. \end{aligned} \tag{C4}$$

Alice can now send the qutrit back to Bob after her unitary transformation and Bob makes a measurement eliminating two out of the four possible states in order to learn either x_0, x_1, or x_2.

Since the state in Eq. (C3) is known to both Bob and Alice, we might ask what changes if Alice prepares the state instead of Bob. She could then apply her unitary transforms or she could straightaway create one of the states in Eq. (C4) (if she is honest). Apart from the fact that Bob randomly obtains either x_0, x_1, or $x_2 = x_0 \oplus x_1$, Alice's cheating probability might then increase, since she may have additional cheating strategies available to her. Similarly, Bob's cheating probability might decrease, since he will have fewer cheating strategies at his disposal. The advantage is that there is no need for entanglement anymore, as was the case in the interactive version of this protocol. Instead of an entangled state of three qutrits, Alice could use a single quantum system; since there are four possible pure states in Eq. (C4), at most four dimensions

would be needed. In this case, the state space is actually only three dimensional. The states in Eq. (C4) have the same pairwise overlaps as the qutrit states in Eq. (9). The reworked protocol (3) therefore becomes equivalent to our XOT protocol in Sec. III. In Sec. III, it is shown that this protocol has the same cheating probabilities as the interactive protocol (3) in Ref. [26]. The price for the noninteractivity is that in the XOT protocol in Sec. III, Bob cannot actively choose if he wants to receive the first bit, the second bit, or the XOR. As we show in Appendix B, however, it is possible to let Bob actively choose b by implementing classical postprocessing.

APPENDIX D: CHEATING PROBABILITIES IN THE REVERSED PROTOCOL

1. Bob cheating in the reversed protocol

Dishonest Bob's aim still is to learn not just one bit but any two of x_0, x_1, or $x_2 = x_0 \oplus x_1$. In the reversed protocol, he wants to know exactly which of the four two-bit combinations Alice has obtained. As in the unreversed protocol, we can consider two scenarios: one where the receiver of the state (now Alice) tests the state and another where the receiver of the state does not test.

a. Alice not testing

When Alice does not test, Bob's optimal cheating strategy is to send Alice the eigenstate corresponding to the largest eigenvalue of one of Alice's measurement operators. Each of the four measurement operators in Eq. (14) is proportional to a pure-state projector and their largest eigenvalues are all equal to $3/4$. Therefore, Bob's highest cheating probability is $B^r_{\mathrm{OT}} = 3/4$, which is the same as his cheating probability in the unreversed noninteractive protocol.

b. Alice testing

When Alice tests, Bob needs to send a state that will pass her test. The testing is analogous to the one applied by Bob in the unreversed protocol. Alice tests a fraction of the states that she receives, to see if her measurement results match Bob's declarations for this fraction of states. She aborts the protocol if there are mismatches and otherwise continues with the rest of the protocol with the remaining states. For the same reasons as earlier, the state that a dishonest Bob has to send, if he wants to pass the test every time, needs to be a superposition of the states that he is supposed to send, entangled with a system that he keeps. This is a state of the form

$$\begin{aligned}|\Phi^r_{\mathrm{cheat}}\rangle = {} & a\,|0\rangle_B \otimes |\phi_{x_0=0}\rangle + b\,|1\rangle_B \otimes |\phi_{x_0=1}\rangle \\ & + c\,|2\rangle_B \otimes |\phi_{x_1=0}\rangle + d\,|3\rangle_B \otimes |\phi_{x_1=1}\rangle \\ & + e\,|4\rangle_B \otimes |\phi_{x_2=0}\rangle + f\,|5\rangle_B \otimes |\phi_{x_2=1}\rangle\,, \end{aligned} \tag{D1}$$

where $\{|0\rangle_B, |1\rangle_B, |2\rangle_B, |3\rangle_B, |4\rangle_B, |5\rangle_B\}$ is an orthonormal basis for the system that Bob keeps and $|a|^2 + |b|^2 + |c|^2 + |d|^2 + |e|^2 + |f|^2 = 1$.

After Alice has made her measurement, Bob's system on his side is prepared in one of four states, depending on whether Alice has obtained 00, 01, 11, or 10. The states that he needs to distinguish between are the pure states

$$\begin{aligned}|\theta_{00}\rangle &= \frac{1}{\sqrt{|a|^2+|c|^2+|e|^2}}\big(a\,|0\rangle_B + c\,|2\rangle_B + e\,|4\rangle_B\big), \\ |\theta_{01}\rangle &= \frac{1}{\sqrt{|a|^2+|d|^2+|f|^2}}\big(a\,|0\rangle_B + d\,|3\rangle_B - f\,|5\rangle_B\big), \\ |\theta_{11}\rangle &= \frac{1}{\sqrt{|b|^2+|d|^2+|e|^2}}\big(b\,|1\rangle_B + d\,|3\rangle_B - e\,|4\rangle_B\big), \\ |\theta_{10}\rangle &= \frac{1}{\sqrt{|b|^2+|c|^2+|f|^2}}\big(b\,|1\rangle_B + c\,|2\rangle_B + f\,|5\rangle_B\big), \end{aligned} \tag{D2}$$

corresponding to Alice obtaining 00, 01, 11, or 10. The states occur with probabilities $(|a|^2 + |c|^2 + |e|^2)/2$, $(|a|^2 + |d|^2 + |f|^2)/2$, $(|b|^2 + |d|^2 + |e|^2)/2$, and $(|b|^2 + |c|^2 + |f|^2)/2$ for $|\theta_{00}\rangle$, $|\theta_{01}\rangle$, $|\theta_{11}\rangle$, and $|\theta_{10}\rangle$, respectively.

In general, it holds that the less equiprobable the states one needs to distinguish between are, the better, since, when one state occurs more often than the others, one can be more certain to guess correctly. Here, the issue for Bob is that if he makes the probabilities of the states in Eq. (D2) more unequal, some pairwise overlaps become larger, i.e., the states are closer together, which makes distinguishing between them harder. Thus, we expect (and are able to prove) that it is best for Bob to choose the constants such that the states are all equiprobable with a probability of $1/4$, e.g., $a = b = c = d = e = f = 1/\sqrt{6}$. Substituting these values into Eq. (D2), the states' pairwise overlaps match the pairwise overlaps of the states in Eq. (9). Thus, $|\theta_{00}\rangle$, $|\theta_{01}\rangle$, $|\theta_{11}\rangle$, and $|\theta_{10}\rangle$ are equivalent to the states in Eq. (9) and Bob's measurement is equivalent to distinguishing between the pure states

$$\begin{aligned}|\phi_{00}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \\ |\phi_{01}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle - |1\rangle + |2\rangle), \\ |\phi_{11}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle - |1\rangle - |2\rangle), \\ |\phi_{10}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle - |2\rangle), \end{aligned} \tag{D3}$$

corresponding to Alice obtaining 00, 01, 11, or 10 and where each state occurs with a probability of $1/4$.

Bob's best measurement is once again a minimum-error measurement. The square-root measurement is optimal, as the states are equiprobable and symmetric. The measurement operators are $\Pi'_{00} = 3/4\,|\phi_{00}\rangle\langle\phi_{00}|$, $\Pi'_{01} = 3/4\,|\phi_{01}\rangle\langle\phi_{01}|$, $\Pi'_{11} = 3/4\,|\phi_{11}\rangle\langle\phi_{11}|$, and $\Pi'_{10} = 3/4\,|\phi_{10}\rangle\langle\phi_{10}|$. With this measurement, Bob's cheating probability B^r_{OT}, when Alice is testing the states that he has sent to her, is

$$B^r_{\mathrm{OT}} = \frac{1}{4}\big[\,\mathrm{Tr}(\rho_{00}\Pi'_{00}) + \,\mathrm{Tr}(\rho_{01}\Pi'_{01}) + \,\mathrm{Tr}(\rho_{11}\Pi'_{11}) + \,\mathrm{Tr}(\rho_{10}\Pi'_{10})\big] = \frac{3}{4}. \tag{D4}$$

We can conclude that our choice for a, b, c, d, e, and f is an optimal choice, since we know that Bob can never cheat with a higher probability when Alice tests a fraction of the states that Bob sends her than he can do when Alice does not test any of his states. Since $B^r_{\mathrm{OT}} = 3/4$ for the case with no tests as well, there is no better way for Bob to choose the constants a, b, c, d, e, and f (there may be other choices that do just as well). The cheating probability for Bob in the reversed protocol is therefore the same as in the unreversed protocol.

2. Alice cheating in reversed protocol

As in the unreversed protocol, a dishonest Alice wants to learn whether Bob has obtained the first or the second bit or their XOR. In this case, however, she is the receiver of the quantum state. Alice will have to distinguish between the three states

$$\begin{aligned}\rho_{x_0} &= \frac{1}{2}\,|\phi_{x_0=0}\rangle\,\langle\phi_{x_0=0}| + \frac{1}{2}\,|\phi_{x_0=1}\rangle\,\langle\phi_{x_0=1}| \\ &= \frac{1}{2}\,|0\rangle\,\langle 0| + \frac{1}{2}\,|2\rangle\,\langle 2|\,,\end{aligned}$$

$$\begin{aligned}\rho_{x_1} &= \frac{1}{2}\,|\phi_{x_1=0}\rangle\,\langle\phi_{x_1=0}| + \frac{1}{2}\,|\phi_{x_1=1}\rangle\,\langle\phi_{x_1=1}| \\ &= \frac{1}{2}\,|0\rangle\,\langle 0| + \frac{1}{2}\,|1\rangle\,\langle 1|\,, \\ \rho_{x_2} &= \frac{1}{2}\,|\phi_{x_2=0}\rangle\,\langle\phi_{x_2=0}| + \frac{1}{2}\,|\phi_{x_2=1}\rangle\,\langle\phi_{x_2=1}| \\ &= \frac{1}{2}\,|1\rangle\,\langle 1| + \frac{1}{2}\,|2\rangle\,\langle 2|\,.\end{aligned} \tag{D5}$$

These mixed states all have prior probability 1/3, since Bob sends each of his six states with probability 1/6. One choice of optimal measurement for Alice has the measurement operators

$$\begin{aligned}\Pi_{x_0} &= \frac{1}{2}\,|0\rangle\,\langle 0| + \frac{1}{2}\,|2\rangle\,\langle 2|\,, \\ \Pi_{x_1} &= \frac{1}{2}\,|0\rangle\,\langle 0| + \frac{1}{2}\,|1\rangle\,\langle 1|\,, \\ \Pi_{x_2} &= \frac{1}{2}\,|1\rangle\,\langle 1| + \frac{1}{2}\,|2\rangle\,\langle 2|\,.\end{aligned} \tag{D6}$$

This gives Alice a cheating probability A^r_{OT} of

$$A^r_{\mathrm{OT}} = \frac{1}{3}\big[\,\mathrm{Tr}(\rho_{x_0}\Pi_{x_0}) + \,\mathrm{Tr}(\rho_{x_1}\Pi_{x_1}) + \,\mathrm{Tr}(\rho_{x_2}\Pi_{x_2})\big] = \frac{1}{2}, \tag{D7}$$

which is the same cheating probability as the one Alice can achieve in the unreversed protocol. Measuring in the $|0\rangle, |1\rangle, |2\rangle$ basis, with $b = i$ corresponding to $|i\rangle$, is another optimal measurement for Alice.

APPENDIX E: EXPERIMENTAL DATA

Here, we present the measurement results of the experiments. The tables contain measured counts C,

TABLE V. The measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when both the parties are honest. $x_2 = x_0 \oplus x_1$.

		Bob					
Alice		Π_A $x_0 = 0$	Π_B $x_0 = 1$	Π_C $x_1 = 0$	Π_D $x_1 = 1$	Π_E $x_2 = 0$	Π_F $x_2 = 1$
$\|\phi_{00}\rangle$	C	166 443	5 562	167 526	719	167 691	1 389
	f	0.3268(7)	0.0109(1)	0.3289(7)	0.00141(5)	0.3292(7)	0.00273(7)
	p_t	1/3	0	1/3	0	1/3	0
$\|\phi_{01}\rangle$	C	167 799	4 375	272	167 383	1 001	166 933
	f	0.3305(7)	0.0086(1)	0.00054(3)	0.3296(7)	0.00197(6)	0.3288(7)
	p_t	1/3	0	0	1/3	0	1/3
$\|\phi_{10}\rangle$	C	4 540	167 803	167 806	446	1 189	168 087
	f	0.0089(1)	0.3291(7)	0.3291(7)	0.00087(4)	0.00233(7)	0.3297(7)
	p_t	0	1/3	1/3	0	0	1/3
$\|\phi_{11}\rangle$	C	3 791	166 615	317	166 221	167 797	1 789
	f	0.0075(1)	0.3289(7)	0.00063(4)	0.3282(7)	0.3313(7)	0.00353(8)
	p_t	0	1/3	0	1/3	1/3	0

TABLE VI. The measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when Alice is cheating. $x_2 = x_0 \oplus x_1$.

		Bob					
Alice		Π_A $x_0 = 0$	Π_B $x_0 = 1$	Π_C $x_1 = 0$	Π_D $x_1 = 1$	Π_E $x_2 = 0$	Π_F $x_2 = 1$
	C	126 264	135 006	124 653	121 434	29	30
$\|0\rangle$	f	0.2488(6)	0.2661(6)	0.2457(6)	0.2393(6)	0.00006(1)	0.00006(1)
x_0, x_1	p_t	1/4	1/4	1/4	1/4	0	0
	C	10	189	127 189	129 235	131 522	121 722
$\|1\rangle$	f	0.000020(6)	0.00037(3)	0.2495(6)	0.2535(6)	0.2580(6)	0.2387(6)
x_1, x_2	p_t	0	0	1/4	1/4	1/4	1/4
	C	130 304	124 349	93	26	119 256	132 601
$\|2\rangle$	f	0.2572(6)	0.2454(6)	0.00018(2)	0.00005(1)	0.2354(6)	0.2617(6)
x_0, x_2	p_t	1/4	1/4	0	0	1/4	1/4

relative frequencies f, and corresponding theoretical probabilities p_t. The digits in parentheses represent one standard deviation at the final decimal place.

In Table V, we show the experimental data for the unreversed XOT protocol when both parties are honest. Alice sends states $|\phi_{00}\rangle$, $|\phi_{01}\rangle$, $|\phi_{11}\rangle$, and $|\phi_{10}\rangle$ and Bob makes an unambiguous quantum state elimination measurement.

In Table VI, we show the experimental data for the case of a dishonest Alice in the unreversed XOT protocol. Alice sends states $|0\rangle$, $|1\rangle$, $|2\rangle$, while Bob honestly makes an unambiguous quantum state elimination measurement.

In Table VII, we show the experimental data for the case of a dishonest Bob in the unreversed XOT protocol. While Alice honestly sends the correct states, Bob applies the square-root measurement. In fact, it also shows the experimental data for the reversed XOT protocol with a dishonest Bob, only interchanging the sender and receiver roles (see names in parentheses).

In Table VIII, we show the experimental data for the reversed XOT protocol when both parties are honest. Bob sends states $|\phi_{x_0=0}\rangle$, $|\phi_{x_0=1}\rangle$, $|\phi_{x_1=0}\rangle$, $|\phi_{x_1=1}\rangle$, $|\phi_{x_2=0}\rangle$, and $|\phi_{x_2=1}\rangle$ and Alice performs a POVM measurement.

In Table IX, we show the experimental data for the case of a dishonest Alice in the reversed XOT protocol. While Bob honestly sends the correct states, Alice performs a projective measurement and classical postprocessing.

TABLE VII. The measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when Bob is cheating. These results also correspond to the reversed protocol with cheating Bob—the roles of sender and receiver are then swapped (see the names in parentheses).

		Bob (Alice)			
Alice (Bob)		Π_{00}	Π_{01}	Π_{10}	Π_{11}
	C	377 482	41 178	38 173	43 299
$\|\phi_{00}\rangle$	f	0.7547(6)	0.0823(4)	0.0763(4)	0.0866(4)
	p_t	3/4	1/12	1/12	1/12
	C	40 908	359 828	52 461	41 808
$\|\phi_{01}\rangle$	f	0.0826(4)	0.7268(6)	0.1060(4)	0.0844(4)
	p_t	1/12	3/4	1/12	1/12
	C	41 904	39 478	378 828	41 595
$\|\phi_{10}\rangle$	f	0.0835(4)	0.0787(4)	0.7548(6)	0.0829(4)
	p_t	1/12	1/12	3/4	1/12
	C	50 901	42 306	38 995	368 643
$\|\phi_{11}\rangle$	f	0.1016(4)	0.0845(4)	0.0779(4)	0.7360(6)
	p_t	1/12	1/12	1/12	3/4

TABLE VIII. The reversed protocol. The measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when both the parties are honest. $x_2 = x_0 \oplus x_1$.

		Alice			
Bob		Π_{00}	Π_{01}	Π_{10}	Π_{11}
	C	249 402	239 442	1 636	1 806
$\|\phi_{x_0=0}\rangle$	f	0.5066(7)	0.4864(7)	0.00332(8)	0.00367(9)
	p_t	1/2	1/2	0	0
	C	3 028	762	249 215	246 373
$\|\phi_{x_0=1}\rangle$	f	0.0061(1)	0.00153(6)	0.4991(7)	0.4934(7)
	p_t	0	0	1/2	1/2
	C	249 097	802	246 042	1 069
$\|\phi_{x_1=0}\rangle$	f	0.5012(7)	0.00161(6)	0.4950(7)	0.00215(7)
	p_t	1/2	0	1/2	0
	C	1 019	241 863	1 840	246 310
$\|\phi_{x_1=1}\rangle$	f	0.00208(6)	0.4926(7)	0.00375(9)	0.5016(7)
	p_t	0	1/2	0	1/2
	C	255 968	38	301	249 572
$\|\phi_{x_2=0}\rangle$	f	0.5060(7)	0.00008(1)	0.00060(3)	0.4933(7)
	p_t	1/2	0	0	1/2
	C	29	237 407	264 287	213
$\|\phi_{x_2=1}\rangle$	f	0.00006(1)	0.4730(7)	0.5265(7)	0.00042(3)
	p_t	0	1/2	1/2	0

TABLE IX. The reversed protocol. The measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when Alice is cheating. $x_2 = x_0 \oplus x_1$.

		Alice		
Bob		$\|0\rangle\langle 0\|$ x_0, x_1	$\|1\rangle\langle 1\|$ x_1, x_2	$\|2\rangle\langle 2\|$ x_0, x_2
$\|\phi_{x_0=0}\rangle$	C	266 828	23	260 337
	f	0.5061(7)	0.000044(9)	0.4938(7)
	p_t	1/2	0	1/2
$\|\phi_{x_0=1}\rangle$	C	266 040	13	261 456
	f	0.5043(7)	0.000025(7)	0.4956(7)
	p_t	1/2	0	1/2
$\|\phi_{x_1=0}\rangle$	C	264 336	255 114	172
	f	0.5087(7)	0.4910(7)	0.00033(3)
	p_t	1/2	1/2	0
$\|\phi_{x_1=1}\rangle$	C	267 393	255 628	151
	f	0.5111(7)	0.4886(7)	0.00029(2)
	p_t	1/2	1/2	0
$\|\phi_{x_2=0}\rangle$	C	1 240	257 057	262 665
	f	0.00238(7)	0.4934(7)	0.5042(7)
	p_t	0	1/2	1/2
$\|\phi_{x_2=1}\rangle$	C	1 192	254 941	262 185
	f	0.00230(7)	0.4919(7)	0.5058(7)
	p_t	0	1/2	1/2

[1] J. Kilian, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88 (Association for Computing Machinery, New York, 1988), p. 20.

[2] Y. Ishai, M. Prabhakaran, and A. Sahai, in *Advances in Cryptology—CRYPTO 2008*, edited by D. Wagner (Springer-Verlag, Berlin, 2008), p. 572.

[3] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, Commun. ACM **28**, 637 (1985).

[4] S. Wiesner, Conjugate coding, SIGACT News **15**, 78 (1983).

[5] M. O. Rabin, How to exchange secrets with oblivious transfer, IACR Cryptol. ePrint Arch. **2005**, 187 (2005).

[6] G. Brassard, C. Crépeau, and J.-M. Robert, in *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)* (IEEE, Toronto, ON, Canada, 1986), p. 168.

[7] G. Brassard, C. Crépeau, and S. Wolf, Oblivious transfers and privacy amplification, J. Cryptol. **16**, 219 (2003).

[8] D. Mayers, Unconditionally Secure Quantum Bit Commitment Is Impossible, Phys. Rev. Lett. **78**, 3414 (1997).

[9] H.-K. Lo, Insecurity of quantum secure computations, Phys. Rev. A **56**, 1154 (1997).

[10] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded quantum-storage model, SIAM J. Comput. **37**, 1865 (2008).

[11] D. Pitalúa-García, Spacetime-constrained oblivious transfer, Phys. Rev. A **93**, 062346 (2016).

[12] D. Pitalúa-García and I. Kerenidis, Practical and unconditionally secure spacetime-constrained oblivious transfer, Phys. Rev. A **98**, 032327 (2018).

[13] C. Crepeau and J. Kilian, in *Proceedings 1988 29th Annual Symposium on Foundations of Computer Science* (IEEE, White Plains, NY, USA, 1988), p. 42.

[14] A. Chailloux, G. Gutoski, and J. Sikora, Optimal bounds for semi-honest quantum oblivious transfer, Chicago J. Theor. Comput. Sci. **2016** (2016).

[15] R. Amiri, R. Stárek, D. Reichmuth, I. V. Puthoor, M. Mičuda, L. Mišta, Jr., M. Dušek, P. Wallden, and E. Andersson, Imperfect 1-out-of-2 Quantum Oblivious Transfer: Bounds, a Protocol, and its Experimental Implementation, PRX Quantum **2**, 010335 (2021).

[16] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[18] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, Bangalore, India, 1984).

[19] S. M. Barnett, *Quantum Information* (Oxford University Press, Oxford, 2009), p. 103.

[20] J. Crickmore, I. V. Puthoor, B. Ricketti, S. Croke, M. Hillery, and E. Andersson, Unambiguous quantum state elimination for qubit sequences, Phys. Rev. Res. **2**, 013256 (2020).

[21] A. Chailloux, I. Kerenidis, and J. Sikora, Lower bounds for quantum oblivious transfer, Quant. Inf. Comput. **13**, 158 (2013).

[22] P. Hausladen and W. K. Wootters, A "pretty good" measurement for distinguishing quantum states, J. Mod. Opt. **41**, 2385 (1994).

[23] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Optimum measurements for discrimination among symmetric quantum states and parameter estimation, Int. J. Theor. Phys. **36**, 1269 (1997).

[24] N. Dalla Pozza and G. Pierobon, Optimality of square-root measurements in quantum state discrimination, Phys. Rev. A **91**, 042334 (2015).

[25] S. Osborn and J. Sikora, A constant lower bound for any quantum protocol for secure function evaluation, arXiv:2203.08268 quant-ph (2022).

[26] S. Kundu, J. Sikora, and E. Y.-Z. Tan, A device-independent protocol for XOR oblivious transfer, Quantum **6**, 725 (2022).

[27] C. Crépeau and M. Sántha, in *Advances in Cryptology—EUROCRYPT '91*, edited by D. W. Davies (Springer-Verlag, Berlin, 1991), p. 106.

[28] R. Stárek, M. Miková, I. Straka, M. Dušek, M. Ježek, J. Fiurášek, and M. Mičuda, Experimental realization of SWAP operation on hyper-encoded qubits, Opt. Express **26**, 8443 (2018).

[29] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter, Minimum-error discrimination between three mirror-symmetric states, Phys. Rev. A **65**, 052308 (2002).

[30] C. L. Chou, Minimum-error discrimination among mirror-symmetric mixed quantum states, Phys. Rev. A **70**, 062316 (2004).

[31] C. Crépeau, in *Advances in Cryptology—CRYPTO '87* (Springer-Verlag, Berlin, 1988), p. 350.